В ПОМОЩЬ РАДИОЛЮБИТЕЛЮ

Патрик Гёлль

Мобильные телефоны и ПК

2-е издание

КОМПАКТ-ДИСК К КНИГЕ

Мобильные телефоны и сети GSM, устройства считывания и компьютерные программы для работы с SIM-картами

ETSF
DUNOD
ДМК ПРЕСС
Издательство

Patrick Gueulle
Ingénieur EFREI

TÉLÉPHONES PORTABLES ET PC

2e édition

DUNOD

ETSF
EDITIONS TECHNIQUES ET SCIENTIFIQUES FRANÇAISES

В помощь радиолюбителю

Патрик Гёлль

Инженер EFREI

МОБИЛЬНЫЕ ТЕЛЕФОНЫ И ПК

Второе издание,
исправленное и дополненное

ДМК
Издательство

Москва, 2004

УДК 621.396.218
ББК 32.884.1
Г31

Гёлль П.

Г31 Мобильные телефоны и ПК / Патрик Гёлль ; Пер. с фр. Брод Т. Е. - 2-е изд., испр. и доп. – М. : ДМК Пресс, 2004. – 232 с.: ил. – (В помощь радиолюбителю).

ISBN 5-94074-223-8

В книге Патрика Гёлля изложены основные принципы построения и работы системы сотовой связи GSM, описывается устройство мобильного телефона и рассказывается об услугах, предоставляемых сетью GSM. Отдельная глава посвящена SIM-картам.

Второе издание дополнено подробным описанием нового инструментария для работы с SIM-картами (BasicCard, BasicSIM), представлено программное обеспечение для считывающих устройств PC/SC. Рассматриваются как специальные программы, которые размещены на компакт-диске, так и имеющиеся на рынке промышленные программные продукты и сопутствующий инструментарий для экспериментов с SIM-картами при помощи ПК. Приводятся схемы и рисунки печатных плат, необходимые для самостоятельного изготовления устройств считывания SIM-карт, а также различных полезных и недорогих аксессуаров к мобильным телефонам.

В приложениях к книге содержатся глоссарий терминов и данные по международному роумингу.

Эта книга предназначена как для радиолюбителей, так и для тех пользователей сотовых телефонов, которые интересуются всевозможными техническими хитростями и оригинальными решениями.

ISBN 2-10-006416-9 (фр.)
ISBN 5-94074-223-8 (рус.)

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

За очень короткий промежуток времени сотовый телефон GSM стал товаром широкого потребления, доступным практически каждому. Отовсюду звучит реклама, предлагающая приобрести эти аппараты иногда совсем недорого.

Подавляющее большинство пользователей мобильных телефонов и не подозревают об удивительной сложности системы сотовой связи. Ведь перед ними чаще всего раскрывается лишь ничтожно малая часть всех ее возможностей. Однако, имея в своем распоряжении компьютер и устройство для считывания чип-карт, можно без особых сложностей заняться исследованием телефонов, их SIM-карт, а также сетей связи различных операторов.

В данной книге рассматриваются вопросы, которые непременно встают перед пользователями, и над которыми им совсем не хочется ломать себе голову. Кроме того, в ней раскрывается множество различных манипуляций, которые операторы и поставщики сознательно «забывают» осветить в сопроводительной технической документации.

Таким образом, эта книга будет полезна многим, как радиолюбителям, так и пользователям сотовых телефонов, – тем, кто интересуется всевозможными техническими хитростями и оригинальными решениями.

БЛАГОДАРНОСТИ

Автор выражает благодарность всем, кто оказал помощь при подготовке к изданию настоящей книги: компаниям Gemplus Card International, L'ETSI, Swisscom Mobile, ZeitControl, Towitoko, Advanced Card Systems, Crownhill Associates, Pipistrel, ELV Electronik, ELEA, а также организаторам замечательного салона CARTES.

И, конечно, «теплый привет» французским операторам, которые нашли возможность установить антенны в нескольких метрах от лаборатории автора.

1 СИСТЕМА GSM

Пользователь мобильного телефона, как правило, не осознает, что он постоянно находится в непосредственном общении с одной из самых сложных систем, когда-либо созданной человеком, – мировой телекоммуникационной сетью. Лет двадцать тому назад так называли международную телефонную сеть, пока ее не обошли Internet и системы наземных и спутниковых мобильных коммуникаций.

Весьма справедливо высказывание одного специалиста, считающего, что для того чтобы поставить на ноги одну единственную систему мобильной телефонной связи GSM, потребовалось приблизительно в десять раз больше усилий, чем отправка человека на Луну. И все же на сегодняшний день мобильный телефон стал прежде всего товаром широкого потребления, относительно дешевым и очень простым в применении.

Хотя резкое увеличение числа пользователей произошло только с конца 1998 года, сама история системы GSM началась в 80-х годах, то есть приблизительно двадцать лет тому назад. Вспомните, в те годы иметь телефон в машине считалось роскошью, будь он рабочим инструментом или забавой, но в любом случае доступно это было лишь очень богатым людям. Однако благодаря развитию и внедрению новых технологий в последние годы произошла значительная демократизация мобильной телефонной связи, так что загруженность используемых частот стала уже угрожающей.

Именно в Европе, а точнее во Франции, некоторые специалисты смогли предугадать это явление приблизительно в то время, когда Ролан Морено изобрел чип-карту. Не исключено, что мобильный телефон в том виде, в котором мы его знаем, обязан большей частью своих возможностей чип-карте, а именно SIM-карте.

1.1. НЕМНОГО ИСТОРИИ

В начале 80-х годов мобильная телефонная связь базировалась, в основном, на аналоговых технологиях, которые, однако, уже становились сотовыми. В каждой стране была разработана своя собственная сеть (например, во Франции – Radiocom 2000), которая оставалась строго национальной, поскольку не обеспечивала никакой возможности общения с абонентами зарубежных сетей.

В настоящее время эти сети закрываются одна за другой, освобождая таким образом частотные диапазоны, которые могут быть использованы значительно эффективнее, обеспечивая более надежную связь.

Вполне вероятно, что первоначально международное сотрудничество было обусловлено размахом предполагаемых инвестиций на исследования и развитие в данной области. Вначале оно было организовано под

эгидой Европейской конференции административных работников почты и телекоммуникаций CEPT (Conférence des administrations Européennes des Postes et Télécommunications) как результат франко-немецкого исследования по вопросу будущего систем мобильной радиосвязи. В 1982 году этот институт объединял 26 европейских стран, а точнее, соответствующие административные учреждения почтовой, телефонной и телеграфной связи PTT (Post, Telephone and Telegraph). Несмотря на то что все данные учреждения были организованы в форме государственных монополий, их руководители все же смогли понять, что очевидная выгода от общеевропейского сотрудничества должна возобладать над национальными интересами.

Таким образом Европейской конференцией и была создана «Специальная группа по разработке мобильной связи», аббревиатура которой (GSM) позднее стала расшифровываться как «Глобальная система мобильной связи» (Global System for Mobile communications). Целью данной группы стала разработка спецификаций общеевропейской сети, не зависящей от национальных границ и способной обслуживать уже миллионы, а не тысячи абонентов. Этот обширный проект, безусловно, сталкивается со всякого рода техническими и экономическими проблемами, а также сложностями в области программного обеспечения, однако все перечисленное несоизмеримо с достижениями, плодами которых мы пользуемся на сегодняшний день.

После признания системы GSM в 1984 году Европейской комиссией Франция, Италия и Германия подписали Соглашение о сотрудничестве от 1985 года. В 1986 году к данному соглашению присоединилась и Великобритания. Уже тогда стало ясно, что разрабатываемая система будет цифровой, идущей в дополнение к «Цифровой сети с интеграцией услуг» – RNIS (Réseau numérique a intégration de services)[1], и что она будет работать в полосе 900 МГц, где для нее были зарезервированы два диапазона по 25 МГц. Но на тот момент все еще не хватало готовности со стороны политических сил, которая могла бы вдохновить производителей.

Под давлением Франции и Германии совещание, состоявшееся в декабре 1986 года, приняло в итоге рекомендацию и указания, направленные на активное развертывание ограниченного спектра услуг системы GSM до 1991 года. В полном масштабе на территории Европы

[1] Более распространенным является англоязычное название данной сети – ISDN (Integrated-Services Digital Network). Далее по тексту будет использоваться именно это обозначение. – *Прим. науч. ред.*

система начала действовать в канун 1993 года, реально введение зон обслуживания продолжалось в течение 1995 года. Также в 1986 году GSM взяла на себя общую ответственность за координацию развития всего комплекса спецификаций.

Оставалось подключить к работе потенциальных операторов, иными словами, будущих разработчиков и владельцев сетей. Этот вопрос решился в сентябре 1987 года, в момент подписания в Копенгагене операторами из 13 стран «Меморандума о взаимопонимании» MoU (Memorandum of Understanding), что соответствовало намерениям в пользу осуществления проекта.

Тем временем во Франции началось тестирование восьми или девяти различных способов передачи радиосигнала, в результате чего неоспоримый выбор пал на метод многостанционного доступа с временным разделением каналов TDMA (Time Division Multiple Access), иными словами, временного уплотнения (мультиплексирования).

Стоит отметить, что решающую роль в разработке данного метода сыграл исследовательский институт CNET, который впоследствии был преобразован во France Télécom.

К февралю 1988 года надежность системы была достаточно доказана, чтобы можно было официально пригласить всех операторов, подписавших «Меморандум о взаимопонимании» для участия в проекте. Но необходимо было довести до конца огромную работу по разработке и тестированию окончательных спецификаций, которые к 1997 году должны были достичь уже 6 000 страниц. Очень скоро стало ясно, что этот титанический труд имеет такой размах и сложность, что дата введения системы в эксплуатацию, назначенная на 1 июля 1991 года, начала ставиться под очень большое сомнение со всеми вытекающими из этого катастрофическими последствиями. Принимая во внимание сложившуюся ситуацию, было принято решение разбить проект на две фазы, дающие возможность запустить систему поэтапно, с некоторым промежутком, хотя на первых порах и не в полном объеме, но вполне функционирующую.

Передача ответственности в 1989 году от группы GSM Европейскому институту стандартов по телекоммуникациям ETSI (European Telecommunications Standards Institute), созданному во Франции, активизировала деятельность, направленную на взаимодействие между административными органами, операторами и производителями, одновременно поставленными в равные условия. В результате «Фаза 1» спецификации GSM была опубликована в 1990 году и принята для разработанной в Великобритании системы DCS 1800 (диапазон 1800 МГц).

В дальнейшем эта система была переименована в GSM 1800. К сожалению, на выставке TELECOM 91, проходившей в Женеве, удалось представить только опытный образец сети. И лишь потому, что на рынке еще не было телефонов GSM из-за нерешенных вопросов совместимости и стандартизации. Надо отметить, что эти телефоны входили в число первого телекоммуникационного оснащения, которое прошло испытания на соответствие единому общеевропейскому стандарту, а не принималось по очереди в каждой стране. Но в 1991 году процедура согласования и стандартизации еще не была разработана.

Наконец, в апреле 1992 года была установлена временная процедура типовых испытаний на соответствие стандарту, позволившая начать массовый выпуск первых сотовых телефонов, что мгновенно стимулировало деятельность операторов.

Все встало на свои места, снежный ком завертелся, и более ничто не могло его остановить.

В июне 1992 года было подписано первое соглашение по роумингу, давшее возможность английским абонентам пользоваться их сотовыми телефонами в Финляндии, а финским абонентам – в Англии. Общеевропейская сеть заработала.

К концу 1993 года насчитывалось уже свыше миллиона абонентов (против более 700 млн в начале 2001 года). А после того, как австралийский оператор Telstra присоединился к остальным участникам Меморандума, система GSM вышла за границы Европы и завоевала весь мир.

На сегодняшний день только во Франции уже около тридцати миллионов абонентов (процент охвата около 50 %), которых обслуживают три оператора.

Мобильные телефоны GSM могут использоваться более чем в сотне стран, разбросанных по всему миру, и даже спутниковые сотовые телефоны работают в соответствии со стандартом GSM.

На смену «Фазе 1» быстро пришла «Фаза 2», а в настоящее время осуществляется реализация «Фазы 2+» и «Инструментария SIM» (SIM ToolKit – STK). Предвестником «третьего поколения» мобильной связи являются WAP-технологии (Wireless Application Protocol – протокол беспроводных приложений) и метод пакетной передачи данных GPRS (General Packet Radio Service); ожидается внедрение UMTS (Universal Mobile Telecommunications System – универсальная система мобильной связи) и полная интеграция с сетью Internet.

Конкуренция на рынке мобильной связи очень высока, что весьма выгодно потребителю. Если постоянно отслеживать новинки на рынке

сотовой связи и проявлять немного настойчивости, можно получить доступ к совершенно невероятным возможностям, причем с довольно небольшими затратами.

Одна из целей данной книги как раз и заключается в том, чтобы показать, чего можно достичь, двигаясь по этому пути.

1.2. СТАНДАРТЫ GSM И ETSI

Выше уже шла речь о том, что отныне всей стандартизацией, связанной с системой GSM, занимается ETSI, в частности, это касается публикации отдельных частей стандарта GSM.

Следует отметить, что за исключением подробной информации о механизмах защиты (например, алгоритмах шифровки), которая доступна только операторам и производителям, подписавшим обязательство о соблюдении конфиденциальности, эти документы не содержат ничего секретного. Каждый может просмотреть каталог, сделать заказ и даже на некоторых условиях приобрести документы, обратившись на сайт ETSI http://www.etsi.org. Необходимо, однако, помнить, что на эту сферу распространяется закон об интеллектуальной собственности.

Данная книга, естественно, не претендует на то, чтобы полностью или частично заменить собой стандарт GSM, который является единственным в своем роде официальным источником. Тем не менее стоит сказать, что при ее написании автор неоднократно обращался к данному стандарту, а также некоторым другим источникам официальной информации, имеющимся в Internet.

Те из читателей, которые захотят пойти еще дальше по пути исследования системы GSM, могут поступить так же, то есть начать с детального изучения стандарта GSM 11.11, а затем воспользоваться поисковыми системами, задав в поле **Поиск** слово «GSM».

Конечно, спецификация GSM не зафиксирована раз и навсегда, и в настоящий момент ведется серьезная работа по подготовке следующих поколений мобильных систем связи, в которых телефония будет представлять, вне всякого сомнения, лишь малую долю всех возможностей.

1.3. СЕТЬ ЦИФРОВОЙ СВЯЗИ

Принципиальное новшество системы GSM по отношению к предыдущим поколениям мобильных телефонов заключается в чисто цифровой природе этой системы. Помимо более эффективного использования спектра радиочастот, цифровая сеть связи позволяет избежать прослушивания разговора каким-либо радиолюбителем или просто любопытствующим, вооруженным сканером.

Тем не менее полезно знать, что в стандарте специально предусмотрены средства для прослушивания каналов связи в профессиональных целях[1] уполномоченными представителями юридических и полицейских органов. Вместе с тем в научных кругах начали циркулировать слухи, что нелегальная дешифровка не столь уж сложна, как это хотелось бы представить.

Цифровая архитектура системы также позволяет использовать огромное множество функций, абсолютно недоступных аналоговым системам.

Строго говоря, сеть GSM должна рассматриваться как беспроводная сеть ISDN, иными словами, как мобильная версия того, что во Франции носит название Numeris. Поэтому совсем не случайно сеть GSM, принадлежащая France Télécom, называется Itinéris.

С учетом вышесказанного сеть GSM наилучшим образом подходит для передачи, помимо речи, различных информационных данных: текстовых и факсимильных сообщений, трафика Internet и т.д.

Сотовый телефон даже самой простой модели представляет собой настоящий микрокомпьютер, мощность которого вполне соизмерима со сложностью и быстротой выполнения возложенных на него задач.

В сочетании с чип-картой (так называемой SIM-картой) он обеспечивает уровень безопасности, которому нет равных, в то время как общеизвестно, сколь незащищенными были аналоговые системы в отношении всяческих незаконных манипуляций.

Качество звука тоже выиграло от применения цифрового метода передачи, хотя и не стоит принимать на веру некоторые утверждения, широко распространяемые с помощью рекламы операторами и производителями телефонов, по следующим соображениям:

- даже очень высокого качества, звук мобильного телефона ни при каких условиях не может соперничать с качеством звука, воспроизводимого с компакт-диска. В лучшем случае он будет эквивалентен звуку, получаемому по обычному проводному телефону;
- поскольку при передаче звука в сотовом телефоне всегда используется цифровой сигнал, то даже если и существуют разные уровни качества получаемого звука (куда входит и звук с высоким разрешением), технически совершенно не оправдано утверждение, что одни модели обладают цифровым качеством звучания, а другие нет;

[1] В России они называются СОРМ – средства оперативно-розыскных мероприятий. – *Прим. науч. ред.*

- цифровая передача сигналов не может быть либо идеальной, либо невозможной. Она может иметь различные недостатки, которые вместе с тем сильно отличаются от недостатков, свойственных аналоговым системам передачи (скорее можно констатировать наличие эха, прерываний или искажений звука, а не свиста или помех).

Наконец, следует иметь в виду, что помехи, которые могут возникнуть от работающего поблизости оборудования (мобильных или стационарных передатчиков), также совершенно отличны от помех, возникающих в подобных условиях от аналоговой передающей аппаратуры.

1.4. СЕТЬ СОТОВОЙ СВЯЗИ

Секрет огромной пропускной способности сети GSM кроется в сочетании двух отдельных технологий:

- цифровой передачи сигналов с применением метода временного уплотнения TDMA;
- сотовой структуры построения сети.

Последнее не относится к новейшим открытиям, поскольку было запатентовано лабораторией Bell Laboratories еще в 1947 году. С тех пор такие структуры широко применялись в аналоговых системах мобильной телефонной связи.

Сотовая структура, без сомнения, является самым оригинальным решением проблемы вечной нехватки радиочастот на территории заданной географической зоны. Идея состоит в ограничении радиуса действия базовых станций таким образом, чтобы частоты, на которых они работают, можно было повторно использовать в других зонах обслуживания абонентов без риска возникновения интерференции (наложения) сигналов.

Но есть и обратная сторона медали: чем меньше будет радиус действия базовых станций, тем больше их потребуется для покрытия заданной зоны обслуживания.

На рис. 1.1 схематически представлен этот принцип. В качестве примера показано, как одиннадцать сот обслуживается при использовании только четырех частот (A, B, C, D).

Однако на практике все обстоит несколько сложнее, поскольку необходимо учитывать множество условий: например, частичное перекрытие сот, близость базовых станций сетей конкурирующих компаний, рельеф местности, степень ее урбанизации и т.д. Все это приводит к тому, что диаметры сот могут варьироваться приблизительно

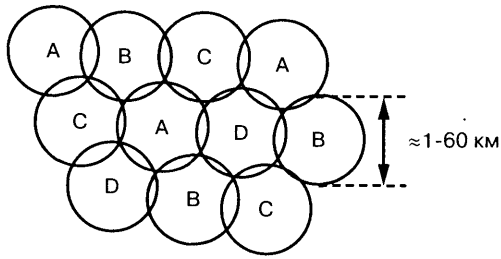


Рис. 1.1. Принцип построения сети сотовой связи

от нескольких сот метров в центре города до нескольких десятков километров в сельской местности.

Естественно, все базовые станции сотовой сети должны быть взаимосвязаны между собой, а также иметь доступ к проводной телефонной сети общего пользования, чтобы абоненты мобильной и стационарной сети могли звонить друг другу. Такое «плетение» сети обеспечивается с помощью либо радиорелейных линий (см. рис. 1.2), либо медных кабельных или волоконно-оптических телефонных линий связи.

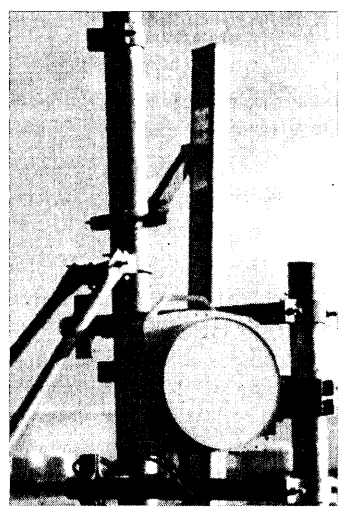


Рис. 1.2. Радиорелейная станция (пропускная способность 2 Мб/с, диаметр параболической антенны 30 см), обслуживающая базовую станцию. На заднем плане – антенна диапазона 1800 МГц

Следовательно, надо отдавать себе отчет в том, что использование мобильного телефона полностью зависит от наличия сети, ее зоны обслуживания, качества функционирования и отсутствия перенасыщения, по крайней мере, в одной сети базовых станций.

При прочих равных условиях можно сравнить мобильные телефоны с усовершенствованными беспроводными телефонами, базы которых превратились из частных в общественные. Такое сравнение тем более справедливо, что технология новых поколений беспроводных телефонов (DECT)[1] многое позаимствовала у технологии GSM.

Очевидно, что мобильный телефон будет работать не везде, хотя операторы и позволяют себе с гордостью утверждать, что коэффициент покрытия составляет 95% (но остается неясным, о чем идет речь, о территории или о населении).

Следует иметь в виду, что на территории, находящейся вне зоны обслуживания (или попадающей в зону неполадок в сети), нет абсолютно никакой возможности поддерживать связь даже с другим абонентом мобильного телефона, расположенным на расстоянии всего нескольких сот метров. И что еще хуже, невозможно обратиться за срочной помощью, набрав номер соответствующей службы (112). В действительности между мобильным телефоном, который является простым терминалом, зависящим от сети фиксированных (базовых) станций, и автономными приемо-передатчиками (как работающими в диапазонах КВ, УКВ или служебной радиосвязи, так и переносными рациями) существует очень мало общего. Это фундаментальное отличие заслуживает того, чтобы заострить на нем внимание.

Между тем, «теневых зон», больших или не очень, довольно много, особенно в малонаселенной местности, где установка базовых станций не представляется достаточно рентабельной.

Зона обслуживания, охватывающая весь земной шар практически без «теневых зон», возможна только при помощи сотовой сети, где роль базовых станций играют... спутники.

Достоинство системы GSM с технической точки зрения заключается в том, что обычно при смене соты связь не прерывается (например, при движении с высокой скоростью на автомобиле или поезде), причем даже при пересечении границы. Однако это в обязательном порядке предполагает, что сеть в любой момент времени

[1] Digital European Cordless Telecommunications – Европейский стандарт на цифровую беспроводную связь. – *Прим. науч. ред.*

«знает», в какой соте находится каждый из мобильных телефонов и может ли он ответить на вызов.

Из этого следует, что теоретически любой включенный мобильный телефон (необязательно тот, по которому ведется разговор) при необходимости может быть локализован с точностью до нескольких сот метров в городе и нескольких километров в сельской местности.

В самом ближайшем будущем можно ожидать появления услуг мобильной связи «третьего поколения», основанных на возможности определения географического положения (автоматизированный поиск гостиниц, ресторанов, такси и т.п.).

1.5. МЕЖДУНАРОДНАЯ СЕТЬ

Как уже говорилось, система GSM с самого начала была задумана как сеть действительно европейского, а значит, и международного масштаба.

С того момента, как к ней примкнули многие страны с других континентов, можно вести речь практически о всемирной сети GSM.

В принципе это должно было бы означать, что любой клиент любого оператора GSM может использовать свой мобильный телефон при перемещениях по всем странам, где имеется соответствующее оборудование, и что он будет всегда доступен по одному и тому же неизменному телефонному номеру (см. рис. 1.3).

Рис. 1.3. Роуминг является одной из наиболее привлекательных возможностей сетей GSM

На практике все зависит от схемы оплаты (идет ли речь об абонементе или о предварительной оплате), выбранной у оператора в своей собственной стране, и наличия возможных международных услуг, бесплатных или оплачиваемых. Также следует учитывать существующие соглашения между операторами различных стран в отношении обмена по предоставляемым услугам.

В лучшем случае действительно удастся облететь весь земной шар, продолжая, как обычно, получать звонки (правда, оплачивая их переадресацию) или текстовые сообщения (бесплатно) и сохраняя возможность звонить практически неограниченно. В худшем случае за рубежом можно дозвониться только, как правило, до службы срочной помощи, набрав номер 112.

Обычно наиболее широкий спектр услуг обходится достаточно дорого, но, прочитав эту книгу, вы узнаете, как можно ими воспользоваться, не имея абонемента, и едва ли с бóльшими затратами, чем при схеме с предварительной оплатой услуг у национальных операторов.

1.6. МОБИЛЬНЫЙ ТЕЛЕФОН В УПРОЩЕННОМ ВАРИАНТЕ

В случае обычной проводной телефонной связи любой телефонный аппарат (соответствующий стандарту) можно просто подключить к любой линии, номер которой ему автоматически сразу же присваивается.

С точки зрения мобильной телефонной связи само понятие «линии» не имеет никакого смысла, и, естественно, не ставится вопроса о том, чтобы каждому абоненту выделить свой радиоканал.

Прежде чем передать вызов, мобильный телефон должен пройти идентификацию у сети, по крайней мере, для того чтобы установить связь.

Наиболее архаичный способ идентификации состоял в том, чтобы просто назвать свой номер телефонистке. Еще совсем недавно именно таким образом моряки, связываясь с землей по радио, звонили домой. Затем на смену пришла автоматизация, и идентификационный номер начал передаваться информационной системе в форме последовательности тональных или импульсных кодовых сигналов.

Невероятная простота, с которой любой желающий мог «присвоить» себе номер абонента, чтобы позвонить за его счет, послужила стимулом для поиска более надежной системы.

В системе GSM мобильный телефон все так же проходит идентификацию у сети в момент своего включения (а затем периодически), но операция выполняется путем закодированного обмена цифровыми

данными. Идентификационные номера и необходимые ключи размещаются на чип-карте, называемой SIM-картой (Subscriber Identification Module – модуль идентификации абонента), которая выдается клиенту оператором.

Достаточно вставить ее в любой мобильный телефон GSM (см. рис. 1.4), чтобы тот сразу же подключил к «линии» владельца SIM-карты. Данному телефону присваивается ее номер, и по ней будет производиться оплата исходящих, а в некоторых случаях и входящих звонков.

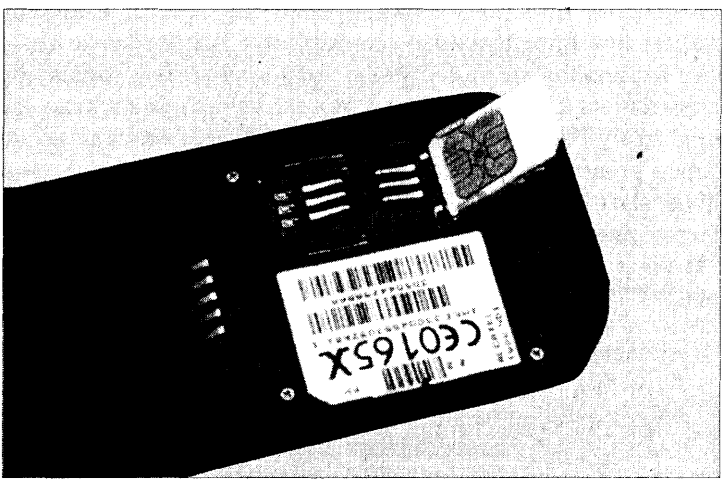


Рис. 1.4. SIM-карта является настоящим «ключом» GSM

Основная цель заключается в полной свободе использования купленного, взятого напрокат или одолженного мобильного телефона в самых разнообразных условиях сегодняшней жизни. Эта заманчивая идея тем не менее сталкивается с суровой действительностью современного мира:

- возможность совершенно свободного использования любого украденного телефона, естественно, привела бы к плачевным результатам;
- предоставление телефонов и аксессуаров к ним по чрезмерно заниженным ценам взамен на приобретение абонемента не может гарантировать, что рано или поздно клиента не переманит конкурирующий оператор;

- полная анонимность мобильного телефона (речь не идет о SIM-карте), вполне очевидно, была бы неприемлема для служб безопасности многих стран, даже тех, в которых гарантируется обеспечение прав и свободы личности.

Поэтому в настоящее время каждый продаваемый мобильный телефон имеет соответствующую электронную «татуировку», состоящую из уникального идентификационного номера (IMEA), который может быть считан сетью в любой момент и при необходимости внесен в ведущийся операторами «черный список». Часто телефон даже бывает «закрыт на ключ» (закодирован) при помощи конкретной SIM-карты или определенным оператором. Тем не менее это не исключает возможности приобрести, хотя и за весьма высокую цену, «не закрытый на ключ» телефон или же получить бесплатно, но приложив к этому серьезные усилия, код вскрытия «замка» по истечении определенного срока использования абонемента.

Наряду с этим ловкие «пираты» часто вскрывают коды мобильных телефонов, лишая их компрометирующего идентификационного номера. Иногда они даже делятся своим маленькими секретами через Internet.

2 СЕТИ

Как говорилось выше, мобильные телефоны полностью зависимы от базовых станций, которые связаны между собой, а также с телефонной сетью общего пользования.

Роль, которую играет сеть GSM, не ограничивается простой передачей сигнала. Она обеспечивает выполнение множества функций, которые превращают ее в огромную информационную систему, где мобильные телефоны выступают в качестве простых терминалов.

Услуги, которые могут быть предоставлены клиентам, в значительной степени определяются возможностями сети каждого из операторов, а не собственно самими телефонами.

2.1. ОПЕРАТОРЫ МОБИЛЬНОЙ ТЕЛЕФОННОЙ СВЯЗИ

С момента появления системы GSM на свет сети мобильной телефонной связи оказались в условиях свободной конкуренции. Тем не менее почти во всей Европе первые сети закрепились за «историческими» операторами, бывшими ранее административными учреждениями в сфере телекоммуникаций. Это объяснялось очень просто: именно они изначально обладали хорошо развитой междугородней инфрастуктурой кабельных сетей и радиорелейных линий, и принадлежащие им приемо-передающие станции часто уже занимали оптимальные местоположения с точки зрения условий распространения радиосигналов, что без проблем позволяло покрывать обширные территории.

Поэтому группы частных лиц, пожелавшие стать операторами сети мобильной телефонной связи, были вынуждены после получения лицензии либо собственными силами создавать межнациональную сеть, либо пойти на довольно невыгодные условия аренды передающего оборудования у своих прямых конкурентов.

Естественно, в ход пошли самые разные способы. Некоторые операторы решили использовать оптоволоконные сети связи, проложенные вдоль железных и скоростных автомобильных дорог, другие – водонапорные башни, имеющие удачное расположение для установки базовых станций.

Как бы то ни было, но времена свершения «подвигов» прошли, и теперь каждый оператор располагает зонами обслуживания, где обеспечивается надежная работа сотовой связи, хотя некоторые операторы специализируются больше на обслуживании городской или сельской местности.

Поскольку некоторые зоны обслуживаются только одним единственным оператором, для оказания на таких территориях содействия

клиентам конкурирующих сетей были подписаны соответствующие соглашения (это также предусматривается в спецификации GSM). Иначе, как это ни странно, например, французы на своей собственной земле обслуживались бы менее качественно, чем иностранные абоненты.

На сегодняшний день можно насчитать около 450 операторов, разбросанных в более чем 120 странах по всему миру. Разумеется, каждый из них обладает своей собственной торговой маркой, а также имеет множество дополнительных, в большей степени «технических» элементов идентификации, о которых полезно знать.

Самым очевидным из них является название сети, которое появляется на дисплее телефона, когда тот готов к выполнению требуемых функций. Например:

- F-ITINERIS или ORANGE – сеть, принадлежащая France Télécom Mobiles;
- F-SFR – сеть, принадлежащая Cegetel;
- F-BOUYGUES, или BYTEL – сеть, принадлежащая Bouygues Télécom.

Отметим, что инициалы страны, стоящие в названии перед именем оператора и написанные через тире или без него, иногда могут быть опущены. Слишком «длинная» надпись также может иногда обрезаться (например, F-BOUYG). Все зависит от программного обеспечения мобильного телефона.

Кроме того, каждому оператору (или сети, что в большинстве случаев является одним и тем же) присвоен свой цифровой код:

- 208-01 – код, принадлежащий Itinéris (сеть под названием ORANGE);
- 208-10 – код, принадлежащий SFR;
- 208-20 – код, принадлежащий Bouygues Télécom.

Как можно догадаться, первые три цифры определяют страну, а две последние соответствуют обозначению самого оператора. Помимо этого, создается впечатление, что возрастающий порядок номеров соответствует появлению все новых операторов на рынке услуг.

Не составляет особой сложности приобрести более или менее актуальный на данный момент список идентификационных номеров сетей во всем мире, посещая Web-сайты операторов, предлагающих своим клиентам возможность использовать мобильные телефоны за границей. В разделе 6.2 приведен полный перечень таких операторов,

предоставленный компанией Swisscom. Ниже представлены некоторые примеры номеров сетей для европейских стран:

- UK-CELLNET 234-10;
- UK-VODAFONE 234-15;
- UK-ONE2ONE 234-30;
- UK-ORANGE 234-33;
- B-PROXIMUS 206-01;
- B-MOBISTAR 206-10;
- B-ORANGE 206-20;
- D1-TELEKOM 262-01;
- D2-PRIVAT 262-02;
- D-E-PLUS 262-03;
- D-VIAG 262-07;
- CH-NATEL D 228-01;
- I-TELECOM 222-01;
- I-OMNITEL 222-10;
- I-WIND 222-88;
- E-AIRTEL 214-01;
- E-RETEVISION 214-03;
- E-MOVISTAR 214-07.

Можно еще указать код 910-03, зарезервированный за спутниковой сетью Iridium, код 222-02, принадлежащий ее конкуренту Globalstar, а также код 001-01, присвоенный вымышленной сети для проведения некоторых тестов.

2.2. ИСПОЛЬЗУЕМЫЕ ЧАСТОТЫ

В сети GSM все операторы делят между собой одни и те же диапазоны частот. Исключение составляют только внутренние сети GSM железнодорожных компаний.

Диапазон GSM 900, который начал использоваться первым, разделен на две группы каналов: восходящие (каналы передачи от мобильного телефона к базовой станции) и нисходящие (каналы передачи от базовой станции к мобильному телефону), которые занимают участки частотного спектра соответственно 890–915 МГц и 935–960 МГц (см. рис. 2.1).

Диапазон, называемый «расширенным», увеличивает стандартную полосу частот GSM 900, однако далеко не все оконечные устройства способны его использовать. История умалчивает о том, что это за особые абоненты, имеющие подобное оборудование и, следовательно, приоритет доступа к соответствующей сети.

Рис. 2.1. Распределение частот в диапазоне 900 МГц

Рис. 2.2. Распределение частот в диапазоне 1800 МГц

Диапазон GSM 1800 (ранее называвшийся DCS 1800), в свою очередь, разделен на участки 1710–1785 МГц и 1805–1880 МГц (см. рис. 2.2).

Американские сети работают на частотах около 1900 МГц (система PCS 1900, или GSM 1900), в будущем предусматривается распространение стандарта GSM на диапазон 450 МГц.

В диапазоне GSM 900 каждый восходящий и нисходящий блок частот разделен на 124 канала (против 374 каналов для GSM 1800). Ширина полосы каждого канала составляет 200 кГц. Для радиотелефонной связи это может показаться слишком большой величиной, но не надо забывать, что речь идет о цифровой передаче, скорость которой составляет 8 × 22,8 Кбит/с при совместной передаче речи и данных. Метод временного уплотнения TDMA фактически позволяет одновременно осуществить восемь соединений на одном канале в соответствии с принципом, представленным на рис. 2.3.

На практике при каждом соединении сигнал сообщения преобразуется в цифровой поток информации (оцифровывается), а затем разбивается на пакеты по 148 бит. На передачу каждого пакета отводится интервал длительностью 0,577 мс каждые 4,616 мс (то есть

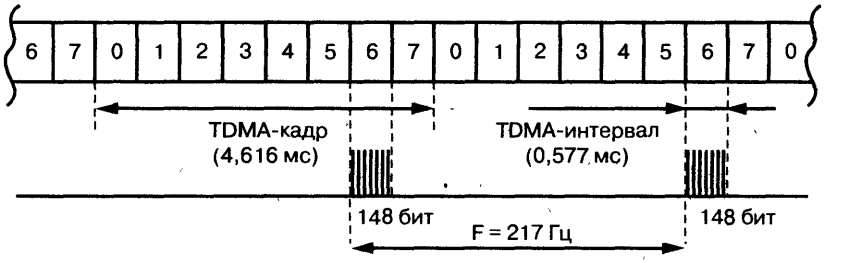


Рис. 2.3. Принцип временного уплотнения TDMA

точно 8 × 0,577). Следовательно, мобильный телефон в режиме соединения выдает пачку очень коротких импульсов каждые 4,616 мс, что соответствует частоте 217 Гц. Именно непосредственным детектированием этих импульсных сигналов и объясняется характерное низкочастотное гудение, которое слышно, когда сотовый телефон используется слишком близко от аудиоаппаратуры, имеющей недостаточно хорошее экранирование.

Благодаря применяющимся в системе GSM цифровым методам невозможно прослушивать телефон GSM при помощи обычного сканера, тем более, что при передаче сообщений присвоение каналов носит динамический характер: во время соединения постоянно происходит переключение (смена) каналов, которое, помимо прочего, приводит к определенному повышению помехоустойчивости при распространении сигналов, особенно в черте города.

Необходимо знать, что радиоволны используемых в системе GSM частот относятся к диапазону ДМВ (СВЧ) и могут распространяться только в пределах прямой видимости.

Как и в случае с волнами, которые применяются в телевидении, естественные и искусственные преграды могут препятствовать распространению радиоволн, ослаблять их в большей или меньшей степени либо отражать.

Обычно сигнал частотой 1800 МГц при распространении обладает более сильным затуханием (примерно в четыре раза) по сравнению с сигналом частотой 900 МГц той же мощности. Соответственно, он имеет и меньшую дальность распространения. Сеть 1800 МГц, таким образом, идеально подходит для обслуживания в городских условиях. При этом используется большое количество базовых станций, обеспечивающих значительную пропускную способность каналов связи.

Сеть 900 МГц, напротив, предпочтительнее для обслуживания больших территорий при использовании меньшего числа радиорелейных (приемо-передающих) станций. Однако в этом случае повышается вероятность перенасыщения сети.

Следует отметить, что длины волн, соответствующие частотам 900 и 1800 МГц, составляют 33 и 17 см. Естественно, это влияет на размеры и эффективность антенн, а также на способность передаваемых сигналов проникать через очень небольшие отверстия, что обычно недоступно для радиоволн.

На сегодняшний день во Франции две компании-оператора GSM 900 уплотняют свои сети 900 МГц, добавляя радиорелейные станции, работающие на частоте 1800 МГц, в зоны с особенно большим потоком трафика. При этом используется технология «bibande» – работа в двух диапазонах. Третий оператор, наоборот, изначально построил свою сеть на 1800 МГц, однако, несомненно, это было вызвано нехваткой частот 900 МГц. Поэтому данной компании пришлось значительно увеличить число мест установки радиостанций. Вместе с тем в зонах с низкой плотностью населения компанией было создано несколько станций, работающих на частоте 900 МГц. Как это ни парадоксально, но именно таким образом оператор, насчитывающий на данный момент наименьшее число абонентов, в результате располагает сетью с наибольшей потенциальной пропускной способностью. Безусловно, это связано и с качеством предоставляемых услуг, и с проведением акций рекламного характера, предлагающих бесплатные услуги связи.

Поскольку во многих странах тоже имеются операторы сетей GSM, работающие в диапазонах 900 и 1800 МГц, вполне понятен интерес к массовому выпуску на рынок двухдиапазонных телефонов, особенно для клиентов, пользующихся услугами всемирного или европейского роуминга.

2.3. СОТЫ И БАЗОВЫЕ СТАНЦИИ

В сотовой сети под «сотой» понимается каждая отдельная зона обслуживания, покрываемая излучением соответствующей основной базовой станции.

В системе GSM каждая сота предназначена для передачи определенного числа каналов, и, следовательно, имеет известный предел пропускной способности.

Таким образом, можно создать соты, которые одновременно будут поддерживать, например, не более восьми соединений.

В каждой соте базовая станция в специально отведенных для этого радиоканалах, или BCCH (Broadcast Control CHannel – канал управления передачей) постоянно передает служебные сигналы идентификации и сигнализации. Поэтому каждый мобильный телефон может путем сканирования (опроса) служебных каналов в любой момент времени располагать списком сот, в большей или меньшей степени покрывающих местность, где он находится, и переходить из одной соты в другую с частотой, позволяющей поддерживать наилучшее качество связи.

Тем не менее необходимо отметить, что, поскольку каждая сота является самостоятельным элементом сети, соты могут отличаться друг от друга по условиям работы и обладать различными недостатками.

На уровне фиксированных станций каждая сота обслуживается антеннами и оборудованием, называемым базовой приемо-передающей станцией BTS (Base Transceiver Station), которое размещается в специальном техническом шкафу (см. рис. 2.4). На рис. 2.5 представлено наиболее часто встречающееся расположение антенн (вид в горизонтальной плоскости), а на рис. 2.6 – внешний вид мачты с размещенными антеннами.

Три сектора, или азимута (направления излучения), определяются в зависимости от местных требований (в частности, от местоположения соседних сот). Каждый сектор покрывается антеннами, ширина диаграммы направленности которых в горизонтальной плоскости составляет около 120°.

Такая конфигурация обеспечивает покрытие зоны обслуживания тремя лучами на все 360°, при этом центр зоны находится в месте расположения передающей станции. Диаметр зоны зависит от мощности передатчиков, а также от ширины диаграммы направленности антенн в вертикальной плоскости, составляющей, как правило, менее 10°.

Кстати, очень часто антенны, размещенные на мачте, имеют небольшой угол наклона, как это показано на рис. 2.7, то есть они слегка наклонены вниз таким образом, чтобы специально ограничить радиус действия передатчиков. Это позволяет, в соответствии со сказанным выше, неоднократно использовать одни и те же каналы на других базовых станциях, находящихся на относительно небольшом расстоянии.

В большинстве случаев каждый сектор оснащается, по крайней мере, двумя приемо-передающими антеннами, состоящими из множества

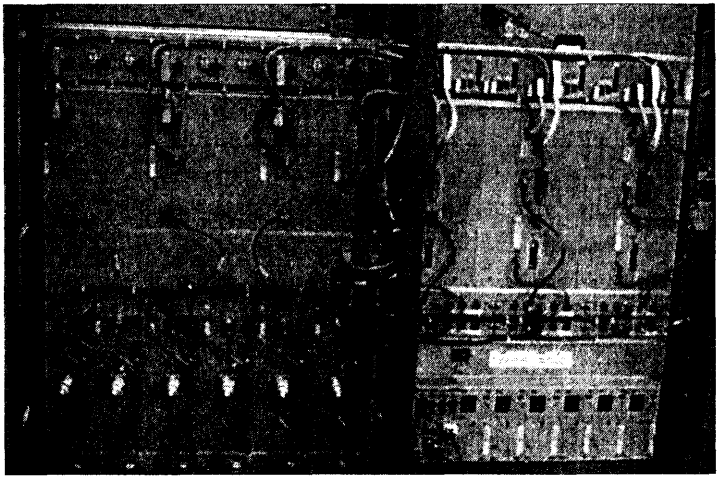


Рис. 2.4. Внутренний вид шкафа BTS фирмы Nortel (слева – передающая часть, справа – принимающая часть)

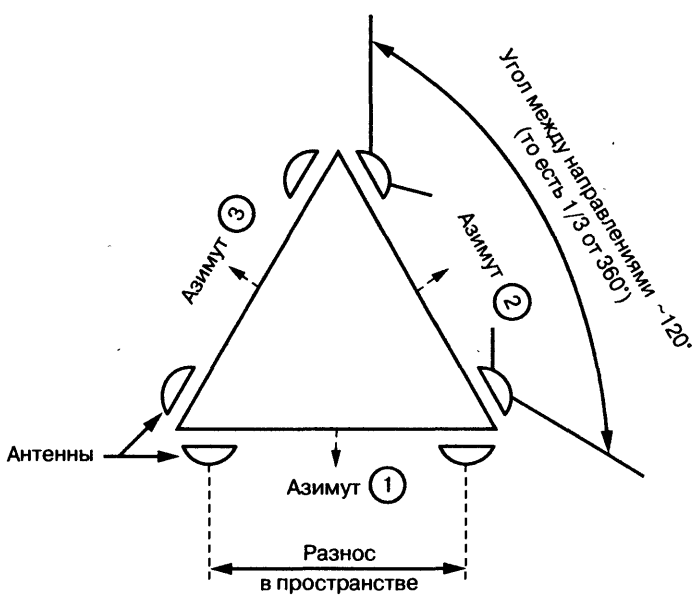


Рис. 2.5. Обычное расположение антенн базовой радиостанции

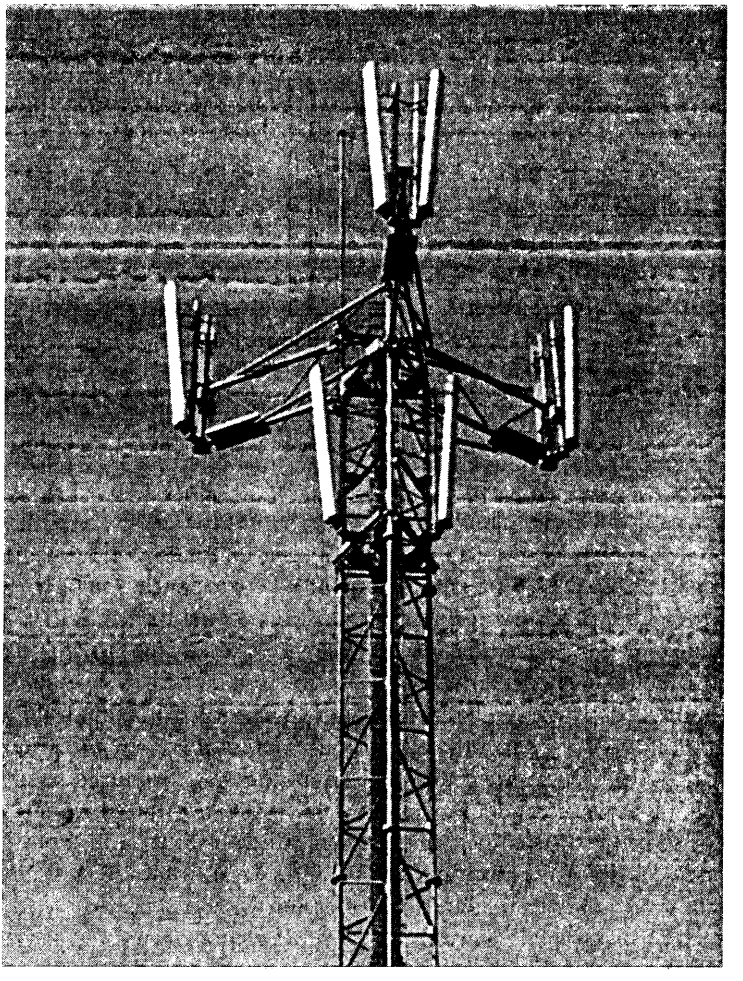


Рис. 2.6. Мачта крупной базовой станции (три сектора, девять антенн)

диполей. Антенны имеют прямоугольную форму и составляют около 2 м в высоту и 10–20 см в ширину. Как правило, они размещаются на расстоянии от нескольких метров до нескольких десятков метров друг от друга, если на мачте или здании имеется для этого достаточно места.

Это расстояние, называемое разнесением, значительно превышает длину используемой волны (более чем на несколько десятков сантиметров) и его вполне достаточно, чтобы условия распространения

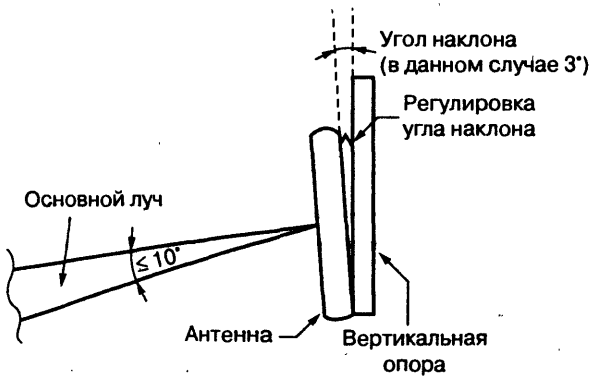


Рис. 2.7. Расположение антенны относительно мачты

сигналов по направлению к одному и тому же мобильному телефону существенно отличались.

Поочередное использование каналов при переходе от одной антенны к другой помогает поддерживать хорошее качество передачи сигналов.

Если место ограничено, то для каждого сектора может быть достаточно и одной антенны. Вместе с тем некоторые фиксированные станции могут быть оснащены антеннами только по двум и даже одному сектору. Как правило, это используется в мобильных станциях, служащих для временного покрытия зон, находящихся вне обслуживания, а также для замены установки, в которой произошел сбой, или для повышения пропускной способности системы, необходимой во время каких-либо чрезвычайных обстоятельств. Внешний вид временной базовой станции (два сектора, две антенны) приведен на рис. 2.8 и 2.9.

Выбор мест расположения радиостанций – достаточно сложный процесс, при проведении которого используют имитацию информационного обмена, исходя из созданных цифровых моделей местности.

Внутри строительных конструкций, которые представляют определенную сложность для покрытия, но являются потенциально рентабельными (например, торговые центры, вокзалы, аэропорты, автомобильные и железнодорожные туннели, многоэтажные здания, где расположены офисы и т.д.), стремятся создать «микросоты», имеющие локальный (ограниченный) радиус действия.

В таких случаях антенны могут быть выполнены из коаксиальных «расщепленных» кабелей, с радиусом излучения, составляющим не

Рис. 2.8. Временная базовая станция, нижняя часть

более нескольких десятков метров. При этом уровень излучения должен быть стабильным, независимо от пути распространения сигнала.

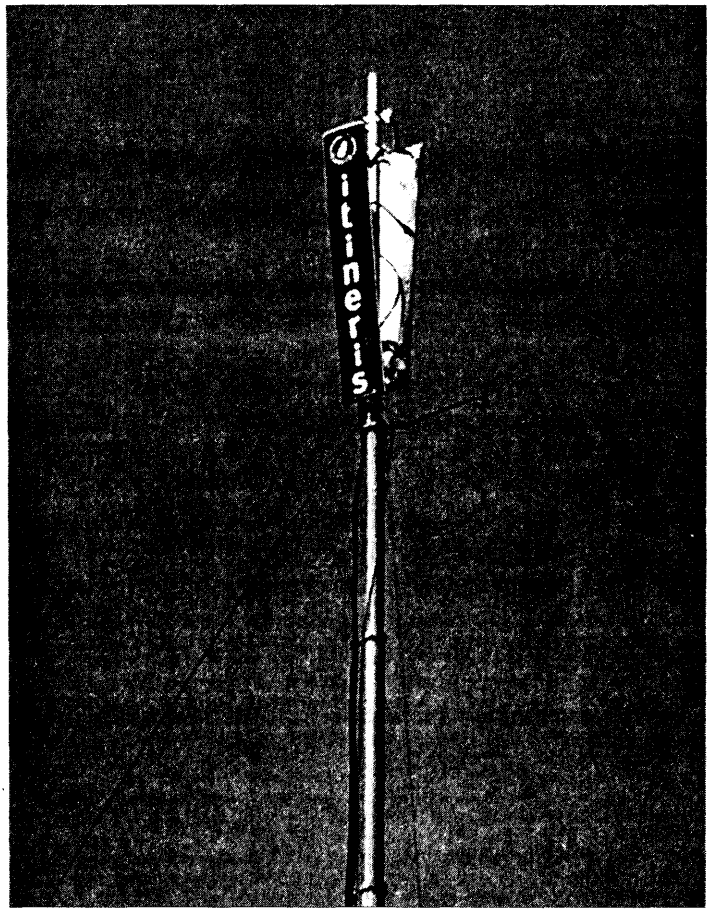


Рис. 2.9. Временная базовая станция, верхняя часть

2.4. МОЩНОСТЬ, РАДИУС ДЕЙСТВИЯ И РАСПРОСТРАНЕНИЕ СИГНАЛА

В сотовой сети радиус действия и базовых, и мобильных станций ограничен, следовательно, мощность работы передатчиков радиостанций относительно невысока.

Что касается GSM 900, то, как правило, передатчики носимых мобильных телефонов обладают максимальной мощностью 2 Вт, а устанавливаемых на автомобили – порядка 8 Вт. Между тем в стандарте определяется четыре класса мощности от 800 мВт до 8 Вт.

Мощность передатчиков мобильных телефонов системы GSM 1800 в два раза меньше, что не может не сказываться на потребляемой энергии, а значит, и на автономности работы «карманных» моделей. Однако радиус их действия значительно меньше, чем радиус действия передатчиков мобильных телефонов GSM 900, который при прочих равных условиях примерно в 16 раз больше.

Несколько сложнее привести порядок величин для мощностей базовых станций, поскольку операторы стараются держать это в секрете. Тем не менее можно сказать, что разброс значений этих мощностей достаточно большой, учитывая разнообразие условий распространения сигналов на местности.

Можно ожидать, что мощность средней передающей станции, работающей в городских условиях и покрывающей зону радиусом приблизительно в 2 км, составляет несколько десятков ватт на сектор (10 Вт = +40 дБмВт[1]). Эта величина имеет место на выходе передатчиков, поскольку благодаря направленному действию антенны мощность излучения (эквивалентная изотропно-излучаемая мощность – ЭИИМ) в заданном направлении может достигать сотен ватт (100 Вт = +50 дБмВт). Приведенные цифры довольно близки к мощности излучения микроволновой печи, работающей с открытой дверцей, и все-таки не сравнимы с сотнями киловатт, излучаемыми в диапазоне FM основными телевизионными и радиовещательными башнями (начиная с Эйфелевой башни, наиболее «грязной» в этом отношении).

В сельской местности эти значения могут быть еще выше за счет установки дополнительных усилителей.

Судя по информации из надежных источников (каталогов изготовителей специальных измерительных приборов), максимальная мощность на выходе передатчика может составлять порядка 30 Вт при работе на частоте 1800 МГц и 300 Вт – на частоте 900 МГц, но на практике не превышает 60–80 Вт. Это может показаться слишком большой величиной, учитывая высокую чувствительность как мобильных, так и фиксированных приемников (не хуже –100 дБмВт для портативной приемной станции хорошего качества). Однако следует принимать во внимание не только потери при прохождении сигнала в свободном пространстве, но и воздействие всякого рода препятствий,

[1] Децибел-милливатт – децибелы, отсчитываемые относительно уровня 1 мВт. – *Прим. науч. ред.*

расположенных между базовой станцией и мобильным телефоном. Например, железобетонные строения способны ослаблять сигналы, проходящие через них (при внутреннем покрытии), в 100–1000 раз (то есть на 20–30 дБ). К числу препятствий можно также отнести кузова автомобилей, кроны деревьев и т.д. Влияние могут оказать и атмосферные осадки.

При отсутствии препятствий ослабление сигнала при распространении возрастает пропорционально квадрату расстояния, увеличиваясь, таким образом, на 6 дБ каждый раз, когда расстояние удваивается.

Следовательно, если спуститься в подземный гараж или в подвал, то ослабление сигнала будет таким же, как и при удалении на расстояние 30 км в пределах прямой видимости.

В связи с исключительным разнообразием условий распространения сигналов было решено, что мощности передатчиков как базовых, так и мобильных станций будут постоянно адаптироваться к текущим условиям (то есть выходная мощность может увеличиваться или уменьшаться). Этим и объясняется тот факт, что автономность работы мобильных телефонов в режиме «разговор» сильно зависит от условий распространения сигнала, и на практике результаты часто оказываются не столь блистательными, как было обещано в рекламе.

Учитывая приведенные цифры, можно сделать вывод, что в идеальных условиях радиус действия будет значительно выше среднего.

Например, при осуществлении связи с моря размер покрываемой береговой зоны такой, что система GSM оказывается значительно эффективнее, чем государственная служба радиотелефонной связи диапазона VHF (ОВЧ). Однако из этого не следует делать вывод, что для обеспечения безопасности на борту корабля достаточно мобильного телефона, поскольку его сигналы не принимаются другими судами, способными оказать помощь. К тому же определить местоположение мобильного телефона гораздо сложнее, чем местоположение радиотелефона. В открытом море не стоит рассчитывать на радиус действия 50 или даже 80 км, который при хороших условиях обеспечивается радиостанциями мощностью 25 Вт. Однако в ясную погоду на побережье Нормандии отлично принимаются сигналы базовых станций четырех английских сетей GSM, находящихся на расстоянии более 120 км.

Этот кажущийся парадокс вызван принципом временного мультиплексирования TDMA, в результате применения которого абсолютный предел радиуса действия системы составляет приблизительно 35 км. Выше уже говорилось о том, что сеть связывается

с мобильным телефоном только в течение интервалов времени длительностью 0,577 мс. При скорости 300 000 км/с радиоволнам потребуется 0,233 мс, чтобы проделать путь 70 км (туда и обратно) между базовой станцией и сотовым телефоном. За пределами радиуса действия 35 км пакеты битов, передаваемые мобильным телефоном, достигают базовой станции в тот момент, когда она уже прекратила их ожидание и перешла на прием сигнала от другого мобильного телефона. Особенно удивительно, когда при постепенном удалении от побережья связь резко обрывается, даже если только что она была отличного качества и дисплей показывает, что режим приема остается оптимальным.

Аналогичное явление может наблюдаться и на суше, в местах, где местность характеризуется пересеченным рельефом. Так, сигнал базовой станции, находящейся на расстоянии свыше 35 км, принимается «четко и ясно» в зоне, которая должна была бы считаться полностью вне диапазона покрытия, поскольку связь с ней невозможна.

Кроме того, может случиться, что, набрав номер 112, чтобы связаться со службой спасения, вы попадаете, например, к пожарным другого департамента. Это совершенно нормальное явление, когда лучше принимается сигнал базовой станции, расположенной на расстоянии 20 или 30 км, чем на расстоянии 2 км, но стоящей за холмом.

Применение различных технических методов позволяет практически удвоить предельный радиус действия системы до расстояния 60 или 70 км, но это может быть сделано только за счет уменьшения пропускной способности базовой станции. В Австралии уже были проведены испытания, подтверждающие данные расчеты. Известно, что некоторые операторы пытались проводить аналогичное тестирование, используя телефоны-автоматы, установленные на паромах.

И наконец, можно вспомнить о «сюрпризах» совсем другого характера, которые могут происходить из-за отражений радиоволн от разнообразных препятствий, включая пролетающие самолеты. Иногда бывает, что мобильный телефон начинает идеально работать там, где это совершенно не ожидалось, например у подножия высокой скалы, но только на протяжении нескольких секунд. В этом случае смещения антенны телефона на несколько сантиметров может быть вполне достаточно, чтобы слышимость резко ухудшилась или прервалась связь.

2.5. ПРОПУСКНАЯ СПОСОБНОСТЬ И НАСЫЩЕНИЕ

Что касается стационарной (фиксированной) или «проводной» телефонной связи, то уже прошли те времена, когда нередко при снятии

трубки приходилось ждать несколько минут до появления сигнала, «приглашающего к набору номера». Теперь каждый абонент располагает парой проводов, связывающих его телефонный аппарат с наиболее близко расположенной станцией, имеющей, как правило, очень большую пропускную способность.

В системе GSM дело обстоит совсем иначе, поскольку мобильный телефон может выйти на связь только в том случае, если сеть сможет отыскать ему свободный интервал TDMA на каналах, имеющихся в зоне обслуживания, где он в данный момент находится. Как известно, диапазон GSM 900 содержит 124 канала, которые распределены между разными операторами.

В лучшем случае, если можно было бы поровну поделить все каналы в одной и той же зоне обслуживания между двумя операторами, это позволило бы одновременно производить только 8 × 62, то есть 496 соединений на оператора.

На практике каждая сота располагает значительно меньшим числом каналов, однако довольно часто оказывается, что в нескольких сотах зоны обслуживания перекрываются.

Положение еще более ухудшается, когда внутри зоны, находящейся на пределе насыщения, устанавливается несколько соединений между мобильными телефонами одной и той же сети.

Ощутимое последствие такой локально ограниченной пропускной способности сетей GSM заключается в том, что при возникновении ситуации, когда в одном и том же месте в одно и то же время собираются многочисленные абоненты мобильных телефонов, перенасыщение сети практически неизбежно.

Самым распространенным примером данной ситуации являются пробки на дорогах, а также массовые мероприятия, собирающие огромные толпы людей, в том числе и в полночь 31 декабря. В подобных случаях единственный способ дозвониться – постоянно набирать номер, что, естественно, еще больше увеличивает нагрузку сети.

Из этого следует, что при возникновении подобных форс-мажорных обстоятельств мобильный телефон оказывается совершенно бесполезным.

Также стоит иметь в виду, что перед ситуацией перенасыщения не все равны, хотя операторы предпочитают об этом не говорить. Особенно показательны результаты сравнительных опытов, проведенных в ночь с 31 декабря 1999 на 1 января 2000 года. Создается впечатление, что абоненты, пользующиеся наиболее дорогими тарифными планами, имеют преимущество перед абонентами с обычными тарифами и особенно

перед пользователями тарифных планов «без абонемента», несмотря на то, что стоимость минуты разговора для последних значительно дороже.

В разделе 02.11 стандарта GSM указано, что любой мобильный телефон принадлежит к одному из десяти возможных классов, каждому из которых в данный момент времени разрешается или не разрешается доступ к сети.

В принципе, принадлежность к тому или иному классу должна быть чисто случайной и использоваться только при нормальном режиме работы сети. Однако на практике весьма сложно проконтролировать, выполняется ли это операторами.

Естественно, специальные классы зарезервированы за некоторыми категориями пользователей, обладающими определенными приоритетами: общественными службами, службой скорой помощи, службой безопасности или самим оператором. В следующей главе будет показано, как определить, к какому классу принадлежит тот или иной мобильный телефон или, точнее, тот или иной пользователь, поскольку эта информация содержится именно на SIM-карте.

Можно еще раз повторить то, что уже было сказано по поводу зоны обслуживания: клиент иностранного оператора, имеющий возможность автоматически или вручную делать выбор между различными операторами сети GSM 900 или 1800 той страны, где он в данный момент находится, будет иметь преимущества по сравнению с абонентами местной сети.

Из этого следует, что быть клиентом иностранного оператора в своей собственной стране выгоднее, когда безопасность и надежность соединения более важна, чем стоимость минуты разговора.

2.6. УСЛУГИ, ПРЕДОСТАВЛЯЕМЫЕ СЕТЯМИ

Эта обширная тема занимает сотни страниц стандарта GSM.

Не имея возможности детально разобрать все предоставляемые услуги, начнем с определения их основных категорий. Потом перейдем к более подробному изучению тех из них, которые позволяют проводить довольно интересные командные манипуляции и вместе с тем весьма скудно отражены в документации.

Передача речи

Основная услуга, предоставляемая каждым мобильным телефоном, а именно передача речи, постепенно уступает место другим видам сообщений, также как и «проводные» линии теперь все больше и больше используются для передачи информационного потока Internet.

Вызов, брошенный GSM, заключался в обеспечении очень хорошего качества звука, несмотря на достаточно невысокую скорость передачи цифровых данных.

После появления методов цифровой обработки временных интервалов проводная телефонная связь уже начала обеспечивать отличное качество воспроизведения речи и даже музыки, хотя при этом полоса пропускания канала связи, как и при передаче аналогового сигнала, по-прежнему составляла всего 3 кГц.

Качество звука во многом определяется используемыми «кодеками» (КОдерами-ДЕКодерами). В этих весьма специфических аналого-цифровых и цифро-аналоговых преобразователях используются алгоритмы преобразования в соответствии с рекомендациями CCITT[1] для проводной телефонной связи и GSM – для мобильной.

Как в одном, так и в другом случае частота дискретизации составляет порядка 8 кГц, но кодеку GSM достаточно скорости передачи данных приблизительно 13 Кбит/с против 64, получаемых при квантовании амплитуды с разрешением 8 бит без сжатия информации (метод ШИМ – широтно-импульсной модуляции). Здесь речь идет о передаче данных на нормальной, так называемой полной скорости FR (Full Rate, англ.), которая при необходимости может быть снижена вдвое для передачи в полускоростном режиме HR (Half Rate, англ.) за счет некоторого снижения качества.

На сегодняшний день основная тенденция состоит в повышении качества звука путем совершенствования методов кодирования при сохранении нормальной (полной) скорости передачи данных. В этом случае речь идет о звуке улучшенного качества при передаче в полноскоростном режиме EFR (Enhanced Full Rate, англ.), звуке высокого качества HQ (Haut Qualité, фр.) или звуке с высоким разрешением HR (Haute Résolution, фр., не следует путать с Half Rate, англ.).

Эти возможности обеспечиваются высокосовершенными электронными компонентами, такими как цифровые процессоры сигналов DSP (Digital Signal Processors), позволяющими получить звук, который по качеству мало чем уступает звуку самых лучших проводных телефонов, даже при работе мобильного телефона в режиме hands free («свободные руки»).

---

[1] Comite Consultatif International Télégraphique et Téléphonique (The International Telegraph and Telephone Consultative Committee – англ.) – Международный консультативный комитет по телеграфии и телефонии (МККТТ), в настоящее время переименован в ITU. – *Прим. науч. ред.*

Надо отметить, что качество звука уже таково, что приходится даже намеренно вводить немного фоновых шумов для заполнения пауз в разговоре, иначе может создаваться впечатление, что соединение прервано.

Однако даже такого очень хорошего качества не всегда бывает достаточно для передачи очень «деликатных» сигналов, которыми, в частности, являются пары «голосовых частот» клавиатуры DTMF (Dual-Tone Multi-Frequency – двухтональный многочастотный набор телефонного номера).

Поскольку такие частоты очень широко используются в разного рода системах дистанционного управления с клавиатуры телефона, то обязательно должна существовать возможность их передачи и с мобильного телефона (эта тема подробно рассмотрена в моей книге «Télécommandes, technique et réalisation»).

Поэтому была разработана система, согласно которой при нажатии в режиме соединения на клавиши клавиатуры соответствующие тональные сигналы DTMF генерируются не мобильным телефоном, а сетью. При нажатии на клавишу телефон отправляет только команду «начало сигнала DTMF», а когда клавиша отпускается – команду «окончание сигнала DTMF». Таким образом обеспечивается прием сигналов пары частот хорошего качества на другом конце соединения без риска микропрерываний и искажений.

Конечно, можно использовать акустическое (звуковое) устройство (например, для связи с автоответчиком) при работе с мобильного телефона, но в этом случае нельзя гарантировать надежность (безошибочность) передачи сигнала.

Вызов срочной помощи

Вызов срочной помощи, собственно говоря, представляет собой особый случай передачи голосовых сообщений. Такого рода звонки являются едва ли не единственным обязательством общественного характера, взятым на себя операторами мобильной телефонной связи. Бесплатное прохождение срочных неотложных звонков гарантирует известную безопасность всякому владельцу мобильного телефона.

Номер 112 является единым для вызова срочной помощи, по крайней мере, в Европе и большинстве других принявших его стран.

Во Франции с помощью этого номера можно также связаться с пожарными департамента, где расположена базовая станция, передающая данный звонок, но это может быть и другой департамент, а не тот,

с территории которого в действительности осуществляется вызов с мобильного телефона.

Если телефон находится в зоне, которая обслуживается его обычным оператором, то последний и обеспечивает передачу данного вызова. Если нет, то эту функцию должны взять на себя операторы других сетей, что еще раз подтверждает преимущество двухдиапазонных мобильных телефонов, дающих максимально возможную безопасность.

В соответствии со стандартом прохождение вызовов по номеру 112 должно обеспечиваться в любой стране, территория которой покрывается сетью системы GSM, с любого мобильного телефона GSM, независимо от того, обладает он действующей SIM-картой или нет.

Однако на практике не все операторы придерживаются данных правил.

Самым уязвимым является тот случай, когда мобильный телефон не имеет SIM-карты и при его включении на дисплее появляется сообщение типа «SIM ABSENT» (SIM-карта отсутствует).

Набор номера 112 (и только этого номера) технически возможен, но передача вызова зависит от доброй воли оператора, призванного его обеспечить. Иначе говоря, как повезет.

Как ни странно, но такой звонок иногда имеет больше шансов дойти по назначению, если он производится с территории, попадающей в зону обслуживания одного единственного оператора, принимающего вызов срочной помощи без SIM-карты, чем в случае, когда на данной местности работают несколько операторов. В последнем варианте мобильный телефон может выбрать сеть с более высоким уровнем сигнала, но при этом нет гарантии, что она обеспечивает прохождение срочных, но анонимных звонков.

Ситуация может упроститься или усложниться в том случае, когда телефон обладает просроченной SIM-картой (например, картой без абонемента, которая не была своевременно продлена, но к которой данный мобильный телефон все еще приписан). Тогда мобильный телефон будет пытаться установить соединение преимущественно с той сетью, с которой он работал до окончания срока действия карты, хотя, как правило, вручную можно перейти к другой сети.

Когда телефон оснащен действующей SIM-картой (что все-таки является самым распространенным случаем), соединение по номеру 112 должно быть выполнено, и, кроме того, будет обеспечена возможность звонить по обычным номерам срочной помощи той страны или стран,

где мобильный телефон зарегистрирован. Таким образом, французский абонент или турист, приехавший во Францию, сможет бесплатно звонить по номерам 15, 17, 18 и иногда 119. За пределами своего государства у иностранного абонента будет возможность позвонить по местным номерам срочной помощи (например, по номеру 999 в Великобритании), только если между сетями соответствующих стран было подписано соглашение по роумингу. В противном случае ему будет доступен только номер 112, и то не всегда.

Следует помнить, что вызовы срочной помощи систематически подвергаются идентификации, даже если обычно мобильный телефон не передает свой номер. Идентификационные номера телефона и его SIM-карты могут быть считаны на расстоянии, предполагается даже возможность географической локализации звонящего.

Это еще один плюс с точки зрения обеспечения безопасности, особенно при нахождении на море и в горах.

Передача данных и факсов

Представляя собой, в сущности, беспроводную сеть ISDN (цифровую сеть с интеграцией услуг), сеть GSM может передавать информационные данные с таким же успехом, как и речь. В настоящее время для этого необходимо соединить мобильный телефон с компьютером, который часто сам является переносным.

В зависимости от типа телефона может потребоваться специальный модем или просто кабель (для подсоединения встроенного программного модема). Возможна даже передача данных в ИК-диапазоне (IRDA – стандарт на передачу данных в инфракрасном диапазоне) через инфракрасный порт. Следующие поколения мобильных телефонов будут обладать более широкими возможностями, вплоть до встраивания упрощенного навигатора Internet или в сами телефоны (с цветным экраном), или в SIM-карты.

На данный момент передача и прием факсов, а также электронных сообщений с помощью мобильных телефонов полностью адаптированы к пока еще относительно низкой скорости передачи данных (2400–9600 бит/с, несмотря на теоретически возможную пропускную способность 22,8 Кбит/с).

Следует отметить, что в любом случае прием и передача данных или факса осуществляется на номер телефона, который отличается от номера, присвоенного для приема и передачи голосовых сообщений. Чтобы иметь возможность воспользоваться указанными услугами, необходимо дополнительно подписаться на специальную услугу

«Передача данных» (Data), которая пока еще не гарантируется клиентам, пользующимся схемой предварительной оплаты.

Передача коротких сообщений

Передача коротких сообщений, которой долгое время пренебрегали, теперь пользуется удивительным успехом (12 млрд сообщений было передано в Европе только за декабрь 2000 года, и 50 млрд сообщений в мире за первые три месяца 2001 года). Такой функции, как обмен небольшими текстовыми сообщениями, содержащими максимум 160 знаков, можно найти весьма разнообразные способы применения, о которых и не думали до появления «третьего поколения» мобильных телефонов.

Данная услуга, называемая передачей SMS-сообщений (Short Message Service – служба коротких сообщений) многое позаимствовала, хотя и на гораздо более высоком уровне, у принципа, который используется в приемниках радиосообщений, или пейджерах.

Телефонные аппараты системы ISDN способны, как известно, принимать короткие сообщения и выводить их на свой дисплей. Аналогичным образом дело обстоит и с мобильными телефонами GSM 900 и 1800. Но поскольку соединение с последними не всегда возможно и их владельцы могут перемещаться практически по всему миру, техническая реализация этого сервиса будет более сложной.

Принцип организации данной услуги построен на том, что сообщения переправляются в единый центр обработки сообщений SMSC (Short Message Service Centre – сервисный центр передачи коротких сообщений) сети GSM. Именно оттуда сообщения доставляются в любое место назначения, как только для этого представится возможность. Это означает, что доставка сообщения происходит при одновременном выполнении следующих условий: включенный мобильный телефон должен находиться в зоне обслуживания сети GSM и иметь разрешение связаться с ней.

До тех пор пока указанные условия не будут выполнены, сообщение хранится в центре SMSC, но не дольше определенного времени, в течение которого данное сообщение действительно. Это время устанавливается отправителем (часто оно составляет 72 часа, но если сообщение имеет срочный характер, то возможно и меньше).

Когда получатель доступен (или с ним можно связаться), обычно требуется всего несколько секунд для того, чтобы после соответствующего звукового сигнала и появления пиктограммы сообщение отобразилось на дисплее мобильного телефона. Тем не менее в случае

длительной перегруженности сетей задержка поступления сообщения в несколько часов и даже несколько дней не должна вызывать удивления.

В зависимости от технических возможностей мобильного телефона может приниматься уведомление о получении, посылаемое в тот момент, когда SMS действительно доходит до адресата. Сообщение будет получено абонентом даже за границей, если он является пользователем услуг европейского или всемирного роуминга. Однако жаль, что в настоящее время некоторые операторы (причем не самая малочисленная их часть) препятствуют прохождению SMS-сообщений от зарубежных центров SMSC.

Несомненно, это объясняется тем, что международная пересылка SMS не требует дополнительных расходов ни от получателя (как правило, прием SMS-сообщения всегда бесплатен), ни от отправителя, который в любом случае потратит таким образом меньше, чем оставив это сообщение в «почтовом ящике» голосовой почты.

Можно считать, что в среднем стоимость отправки одного короткого сообщения не должна превышать 0,5–1,0 франка[1] (будьте внимательны при округлении во время перевода в евро). Себестоимость передачи SMS составляет для оператора совсем ничтожную сумму, так как для этого трафика задействуются каналы, отличные от используемых при голосовых сообщениях (передача осуществляется по «сигнальным» каналам, гораздо менее загруженным).

Каждый центр обработки сообщений идентифицируется международным номером вызова, похожим на номер мобильного телефона. Вот несколько примеров:

- +33609001390 (SFR);
- +33689004000 (Orange);
- +33660003000 (Bouygues Télécom);
- +41794999000 (Swisscom).

Если такой номер набрать на обычном телефоне, то последует голосовое сообщение типа «Такого номера не существует». Эти номера доступны только с мобильного телефона GSM и только при наличии в меню возможности программирования параметров SMS.

---

[1] На данный момент в России, например, в сети оператора Би-Лайн стоимость отправки одного SMS-сообщения составляет 0,05–0,07 доллара. – *Прим. науч. ред.*

Впрочем, каждый оператор может отказать в доступе с других центров SMSC, кроме собственных, совсем близко расположенных от клиентов. Часто оказывается, что гораздо выигрышнее в своей стране быть клиентом зарубежного оператора.

Между тем существуют своего рода «мостики», до которых можно дозвониться и по обычной телефонной сети с помощью модема по различным номерам (например, + 41794998991 для совместимого с ПК доступа к VT100 компании Swisscom).

Существуют разные протоколы для доставки SMS-сообщений в центры передачи по цене, включающей только плату за соединение с обычного проводного телефона. Хотя можно найти программы, позволяющие достичь этих «мостиков» с обычного ПК, намного проще использовать для этой цели Internet. Некоторые операторы предлагают бесплатную отправку SMS-сообщений с их Web-сайтов только для своих абонентов, иногда даже с получением подтверждения по электронной почте, когда сообщение действительно достигнет порта назначения.

Некоторые независимые сайты позволяют бесплатно отправлять SMS-сообщения, но довольно часто за счет размещения своей рекламы. В то же время различные зарубежные Web-сайты операторов GSM (например, http://www.mtnsms.com/sms/) предоставляют возможность бесплатно отправлять SMS-сообщения абонентам из многих стран. Можно только удивляться тому, как часто лучшая услуга предоставляется, причем бесплатно, оператором с другого конца света, а не тем, кому вы платите за абонемент. В этом, впрочем, кроется причина мистического исчезновения SMS-сообщений зарубежного происхождения.

Однако использование коротких сообщений выходит далеко за рамки обычного соединения между абонентами. На этой надежной и недорогой системе основана работа различных информационных служб (биржевых, метеорологических, службы новостей, сообщений о ситуации на дорогах и т.д.). Среди них есть и платные, и бесплатные.

Сами операторы охотно применяют эту систему для информирования клиентов, пользующихся формой предварительной оплаты, о том, каким кредитом те располагают, а также для предупреждения о поступлении сообщения в «почтовый ящик» голосовой почты. Таким же образом распространяется рекламная информация, тексты приветствия для иностранных туристов и передаются необходимые данные для изменения параметров SIM-карты или телефона (конечно, более конфиденциальным образом).

Успешным применением данной услуги является дистанционная загрузка персональных мелодий звонков, коллекции значков или списков телефонных номеров.

Хотя Internet-услуги мобильной связи «третьего поколения» пока не реализованы, но уже сейчас существуют интересные возможности для приема и отправки электронной почты при помощи SMS, при этом расходы на данный вид услуг относительно невелики. Заметим, что при определенных условиях 160-символьный предел может быть обойден путем «конкатенации» (сцепления) нескольких SMS в одно сообщение длиной до 640 знаков.

В заключение добавим, что SMS-сообщения нашли применение в различных областях промышленности для систем дистанционного управления и наблюдения за отдаленной местностью.

Дополнительные услуги

Именно дополнительные услуги значительно расширяют круг возможностей сетей и мобильных телефонов GSM. Стандарт GSM определяет спектр услуг, способных удовлетворить большинство требований пользователей.

В число предлагаемых услуг входят такие, как ответная отправка звонков (включая голосовые сообщения и автоответчик), запрещение звонков определенного типа, представление входящих номеров и двойной вызов.

Важно отдавать себе отчет в том, что данные услуги предоставляются сетью, а не мобильным телефоном, несмотря на то что последний обеспечивает требуемый уровень совместимости. Из этого следует, что каждый оператор свободно может предложить или не предложить ту или иную дополнительную услугу всем своим клиентам или только какой-то их части, бесплатно или на платной основе.

На самом деле роль мобильного телефона состоит прежде всего в том, чтобы дистанционно активировать, дезактивировать и задавать параметры услуг, предлагаемых сетью. Это осуществляется посредством выполнения функций, предусмотренных в меню телефона, или прямым набором специальных кодов. Например, чтобы активировать функцию «двойной вызов», предлагаемую сетью, надо набрать *43#, чтобы ее дезактивировать – #43#, а можно набрать *#43#, чтобы запросить сеть, имеется ли вообще такая услуга.

В сущности, это очень похоже на процедуру, которая применяется для управления дополнительными услугами обычной проводной

телефонной сети (например, чтобы дезактивировать перенос звонка, следует набрать #21#).

Отчет о выполнении команды будет отображен на дисплее телефона.

Необходимо помнить, что логическая схема каждого мобильного телефона анализирует любые номера и команды, набираемые на его клавиатуре, чтобы точно определить, какие действия требуется выполнить. Если просто набран номер телефона, то сразу после нажатия кнопки подтверждения будет установлено соединение.

Может быть введен код команды, которая должна быть выполнена локально, самим телефоном, причем информация об этом в сеть не передается. Например, при наборе *#06# (даже без подтверждения) на дисплей телефона выводится его идентификационный код IMEI (International Mobile Equipment Identity – международный идентификационный номер мобильного устройства), который, естественно, должен соответствовать номеру, указанному на наклейке телефона и упаковке.

Другие команды, которые будут рассмотрены ниже, позволяют разблокировать SIM-карту в том случае, если три раза подряд был введен ошибочный конфиденциальный код. Кроме того, что еще более интересно, с их помощью можно получить доступ к «скрытым меню», предназначенным только для служебного использования техническими специалистами.

Как только телефон распознает стандартный код дополнительной услуги, он приступает к совместной с сетью процедуре активации, дезактивации или проверки функционирования. Помимо точно оговоренных случаев, другие сочетания набираемых знаков рассматриваются мобильным телефоном как код нестандартной дополнительной услуги USSD (Unstructured Supplementary Service Data – неструктурированные данные дополнительных услуг).

Если мобильный телефон поддерживает такую функцию, то последовательность набранных знаков передается в «прозрачном» режиме оператору, выдавшему установленную в данном телефоне SIM-карту. Это происходит всегда, находится ли абонент в своей стране или за ее пределами, пользуясь услугами иностранной сети.

Например, код *147*# позволяет владельцу международной карты с предварительной оплатой (в частности, карты GSM CARD easyRoam компании Swisscom) бесплатно получить поступающую из Швейцарии информацию о сумме кредита, оставшейся на оплату соединений. Эти данные выводятся на дисплей телефона в виде текстовых сообщений.

В действительности функция USSD является двусторонней, позволяющей операторам посылать подобные сообщения своим клиентам независимо от сети-партнера, которая их обслуживает.

Операторы обладают полной свободой действий в том, чтобы предлагать или не предлагать как услуги, предусмотренные стандартом, так и свои собственные услуги, предоставляемые по специальным кодам. Если SIM-карта и мобильный телефон поддерживают SIM-инструментарий (SIM Toolkit – STK), возможно даже создание дополнительных меню, перехват и частичное изменение последовательности данных пользователя (направление SMS-сообщений по «короткому пути» местного оператора, функции типа «обратного вызова» и т.д.). Это позволяет операторам навязывать свою коммерческую политику, особенно не беспокоясь о соблюдении добрых намерений стандарта GSM.

Можно привести простой пример, когда некоторые операторы «забывают» предусмотреть дезактивацию услуги голосовых сообщений и автоответчика с мобильного телефона (обычно данная операция выполняется при наборе ##002#). Некоторые тарифные планы прямо предписывают постоянное активирование службы сообщений (незачем убивать курицу, несущую золотые яйца). Другие операторы предоставляют возможность дезактивировать эту услугу только посредством обращения в центр обслуживания клиентов, причем связаться с центром можно только по номеру телефона, соединение с которым оплачивается по повышенному тарифу, а пауза ожидания с музыкальным сопровождением длится, на удивление, исключительно долго.

Решение, принимать или не принимать все эти капризы, остается за потребителем. В конце концов, можно всегда заменить оператора, действия которого по оказанию дополнительных услуг представляются недостаточно оправданными.

На рынке услуг сотовой связи существует достаточно оживленная конкуренция (как на международном, так, кстати, и на национальном уровне), позволяющая каждому владельцу мобильного телефона выбрать то, что ему действительно требуется, а не то, что ему навязывают.

2.7. РЕГИСТРАЦИЯ МОБИЛЬНЫХ ТЕЛЕФОНОВ

При включении мобильный телефон должен сообщить сети, в какой соте он находится, чтобы можно было переправлять туда предназначенные ему звонки и сообщения.

Кроме того, необходимо, чтобы мобильный телефон предоставил сети данные о том, что абонент имеет право пользоваться этими услугами и что они будут оплачены.

Во время процесса инициализации (установки в исходное состояние) телефон сканирует все каналы в диапазонах частот, которые он способен принимать. В результате данной процедуры создается список операторов, охватывающих зону, в которой находится абонент, и выясняется, есть ли в этом списке код его «домашней» сети. В случае положительного ответа мобильный телефон определяет соту, расположение которой лучше всего подходит для обслуживания, и сообщает ей свои данные.

Если оператор признает подлинность SIM-карты, то он приступает к проверке ее прав в своей собственной базе данных (срок действия абонемента или предварительно оплаченных услуг) и запускает процесс идентификации, основанный на криптографическом подходе.

Если все в порядке, то он регистрирует мобильный телефон в качестве действующего в рассматриваемой соте. Начиная с этого момента сеть отслеживает перемещения мобильного телефона и при необходимости принимает решение о смене соты (handover – передача обслуживания) для поддержания хорошего качества связи и непрерывного трафика. Появление на дисплее мобильного телефона имени оператора свидетельствует о выданном разрешении на соединение.

Этот процесс значительно усложняется, когда мобильный телефон не может найти сеть, к которой приписан. Если имеется другая сеть или несколько сетей, возможно, даже определенных как «предпочтительные» в SIM-карте, то при условии, что функция «автоматической регистрации» активирована, телефон может попытаться зарегистрироваться у них.

Успешная регистрация, как правило, говорит не о том, что владелец мобильного телефона находится на территории своей страны, а о том, что удалось найти сеть, которой разрешил воспользоваться его обычный оператор.

В регистрации отказывается в том случае, если в своей собственной стране мобильный телефон находит только сеть конкурентов, или когда за границей он не имеет доступа к услуге международного роуминга, действующей на данной территории. Во избежание повторных обращений к недоступной сети (за исключением звонков вызова срочной помощи) мобильный телефон отмечает этот отказ в списке запрещенных сетей, который он ведет на своей SIM-карте.

Ниже будет показано, как изменить или даже аннулировать этот список. Тем не менее необходимо помнить, что в мобильных телефонах в обязательном порядке предусматривается возможность принудительно (в ручном режиме) активизировать попытки зарегистрироваться в любой сети, даже в той, которая считается запрещенной.

Режим работы, который значительно изменяется от одной модели телефона к другой, описан (однако часто очень кратко) в руководстве по пользованию.

Эта возможность выбирать сеть предлагается как в том случае, когда устанавливается потерянный контакт с последней используемой сетью, так и если телефон конфигурируется в режиме «ручной регистрации». Если какой-либо выбор не осуществлен, то мобильный телефон просто продолжает попытки вновь зарегистрироваться в сети, которая использовалась последней.

Процедура отключения мобильного телефона от напряжения питания в значительной степени подобна той, которая только что была рассмотрена.

Снятие с регистрации является неотъемлемой частью процедуры прекращения работы «самим» мобильным телефоном. Прежде чем полностью отключить питание всех своих внутренних схем, телефон должен сообщить об этом сети.

То же самое происходит, когда телефон выходит из зоны радиуса действия соты, не найдя при этом другой, способной продолжить обслуживание, если только потеря контакта не была слишком резкой и осталось время на снятие с регистрации.

Другая нестандартная ситуация возникает, когда питание мобильного телефона отключается из-за резкого удаления батареек. Если на снятие с регистрации не остается времени, то телефон бесследно «исчезает» из поля зрения сети.

Телефон будет обнаружен вновь, только когда на мобильный снова будет подаваться напряжение питания и он заново зарегистрируется у той или иной сети.

2.8. АВТОМАТИЧЕСКАЯ НАСТРОЙКА НА МЕСТНУЮ СЕТЬ СВЯЗИ, ИЛИ РОУМИНГ

Речь, без сомнения, идет об одной из самых удивительных возможностей мобильных телефонов GSM, позволяющей их владельцам ездить по всему свету и при этом продолжать пользоваться своими

телефонами как обычно. Как и все дополнительные услуги, данная услуга предлагается оператором и, естественно, имеет свою цену.

Пользование сетью зарубежного оператора предполагает наличие действующего соглашения между ним и оператором, клиентом которого является владелец телефона. Большинство данных соглашений являются взаимными, и в целом между операторами со всех концов света их насчитывается около 20 000.

К началу 2000 года благодаря такому режиму работы обеспечивалось около 400 миллионов соединений в месяц.

Следует отметить, что в случае французских департаментов, расположенных за пределами европейского континента и обслуживаемых специальными операторами, речь также идет о роуминге, даже если прием и передача звонков континентальных абонентов производится без особых формальностей.

Качественное функционирование роуминга предполагает ведение сложного, быстрого и безопасного обмена данными между операторами со всего света.

При включении на территории зоны обслуживания «гостевой» сети мобильный телефон пытается зарегистрироваться у местных сетей, доступных либо по уровню качества приема, либо согласно списку предпочтительных сетей, запрограммированному в его SIM-карте.

Каждая сеть при опознавании иностранной SIM-карты сначала определяет, какой стране и какому оператору принадлежит данная SIM-карта, а затем отправляет последнему запрос на аккредитацию.

Ответ, который, как правило, занимает лишь несколько мгновений, может быть положительным или отрицательным и даже условным (в последнем случае предусматриваются некоторые ограничения, например запрет некоторых видов соединений).

Если ответ носит положительный характер (иначе говоря, клиент пользуется услугой международного роуминга, действующей на данной территории), то местный оператор переходит к регистрации мобильного телефона, после чего имя оператора появляется на дисплее. Кроме того, мобильному телефону присваивается временный конфиденциальный местный номер, о котором сообщается исключительно оператору клиента.

С этого момента владелец телефона начинает получать звонки, адресованные по его обычному номеру, причем звонящие и не догадываются о том, что данный абонент находится в путешествии (если

только они не заметят тонких отличий в ритме звонка). При этом счет путешественника возрастет на величину стоимости переадресации звонков на его временный номер.

Счет за звонки, сделанные с мобильного телефона, будет выставлен местным оператором (по действующему в этой стране тарифу) оператору, выдавшему SIM-карту, который, в свою очередь, представит счет своему абоненту, добавив при этом свой процент.

Операции по расчетам чаще всего производятся не в режиме реального времени, а группируются и выполняются один раз в день. Аналогично обработке, которой подвергаются банковские чеки, эти операции включают механизмы финансовой «компенсации» между операторами и происходят, в основном, на территории Швейцарии.

Создается впечатление, что эти тонкости с задержкой оплаты соединений являются причиной определенного типа мошенничества, что объясняет желание операторов обезопасить себя со всех сторон, но иногда мало устраивает клиентов.

Всех этих неудобств можно избежать, если найти оригинальные пути использования технических возможностей, предлагаемых системой GSM, например, применив процедуру call-back (обратный вызов) к звонкам, сделанным из-за границы. Ниже будет подробно рассмотрен принцип работы международной карты с предварительной оплатой, функционирующей подобным образом.

2.9. ПРИНЦИПЫ ТАРИФИКАЦИИ

Всего лишь несколько лет назад единственным способом получить доступ к сети мобильной телефонной связи было приобретение абонемента у оператора или компании, занимающейся продажей подобного рода услуг. В обмен на получение телефона часто по исключительно низкой цене клиент на определенный срок давал разрешение на неограниченное взимание сумм со своего банковского счета и очень часто значительно переплачивал.

Придумав форму оплаты без абонемента, иначе говоря, с предварительной оплатой, операторы и не предполагали, что она будет пользоваться большой популярностью у клиентов, подписывающих «пустые» (не обеспеченные денежным покрытием) чеки. В большинстве стран более половины клиентов, выбравших способ предварительной оплаты, продолжают отдавать ему предпочтение и в дальнейшем, при этом часто месяцами не пользуясь телефоном. Такое

положение дел, естественно, заставляет операторов волноваться за свои доходы. Поэтому они пытаются либо отговорить потребителей от подобных форм оплаты, либо побуждают их всеми возможными способами тратить все больше и больше.

Принцип оплаты таков: цена SIM-карты (или полного пакета услуг) включает определенный кредит на соединения, который можно использовать, просто предъявив идентификационный номер пользователя (фактически – покупателя). Когда кредит израсходован (или истек срок пользования этим кредитом), то следует просто произвести его пополнение, при этом не надо ни контракта, ни аванса, ни счета и, самое главное, никаких снятий со счета!

Обычно можно не пополнять свой счет в течение нескольких месяцев, на протяжении этого периода сохраняется возможность принимать звонки и короткие сообщения, а также, конечно, обращаться по номерам срочной помощи. Тем не менее по истечении этой отсрочки номер соответствующего телефона будет окончательно потерян, однако это никоим образом не препятствует возможности звонить по номеру 112.

Аналогичными привилегиями сегодня иногда пользуются телефоны, предлагаемые вместе с картами предварительной оплаты, которые на протяжении длительного времени продавались дороже, чем телефоны в рамках других схем оплаты.

Конечно, такие телефоны «запираются» сопровождающей их SIM-картой, хотя код «отпирания» может быть получен бесплатно через шесть месяцев после начала использования (активирования) счета, иначе говоря, даже раньше того, как счет будет пополнен в первый раз.

2.10. ПРЕДОПЛАЧЕННОЕ «ПУТЕШЕСТВИЕ»

Использование за границей национальных тарифных схем предварительной оплаты будет оставаться настоящей головоломкой до тех пор, пока технология, называемая «CAMEL» (Customized Applications for Mobile network Enhanced Logic), не станет общепринятой. Она позволяет получать доступ из-за границы к специальным услугам своего местного оператора (пополнение счета, извещение о кредите, доставка сообщений и т.д.) и получать отчет о них в реальном времени.

Понятно, что сначала приветствие (сигнал подтверждения) поступает от операторов международного масштаба, то есть тех же потенциальных операторов, которые обслуживаются в сетях своих партнеров.

Специалисты компании-оператора Swisscom Mobile, считающей себя обладателем наибольшего числа соглашений по роумингу, нашли изящное решение сложной проблемы предварительной оплаты звонков, сделанных из-за границы. Их карта GSM CARD easyRoam (см. рис. 2.10), специально предназначенная для клиентов из разных стран, также как и карты для ее пополнения (так называемые value cards) продаются через Internet (http://www.easy-roam.com).

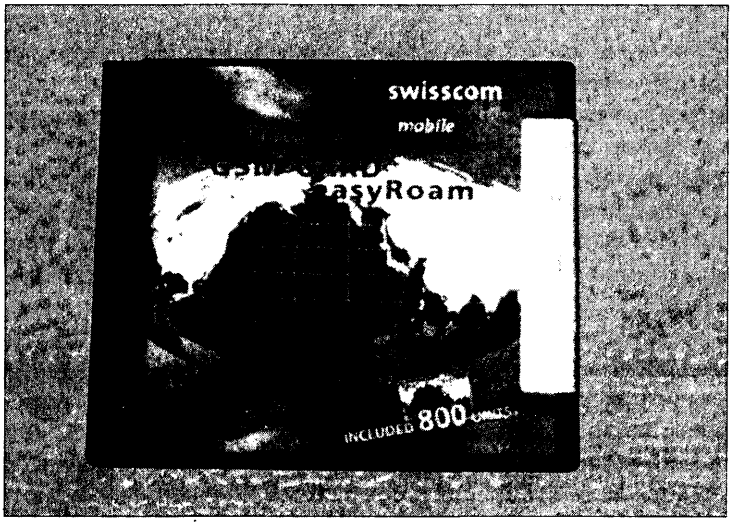


Рис. 2.10. Комплект GSM CARD easyRoam компании Swisscom

Будучи оригинальным применением функции нестандартной дополнительной услуги USSD, карта работает в некотором роде дистанционно. Благодаря добавлению коротких префиксов, начинающихся со звездочки, все набираемые пользователем номера и коды напрямую передаются в Швейцарию, а не подлежат интерпретации и выполнению местным оператором.

Для того чтобы позвонить, например, по номеру + 33 1 22 33 44 55 (то есть в международном формате 01 22 33 44 55), следует набрать *111*33122334455#.

Как только такой запрос на звонок будет получен, кредит имеющихся на карте единиц начинает контролироваться и ретранслироваться на дисплей мобильного телефона. Если сумма кредита достаточна, то мобильный телефон сразу же вызывается (раздается звонок), но соединение устанавливается (и оплачивается) только с момента, когда владелец отвечает.

Таким образом, и вызывающему, и владельцу вызываемого телефона звонят с территории Швейцарии, что позволяет исключить из процесса местного оператора и его особенности тарификации. Соединение в режиме реального времени, при полной безопасности и без неприятных сюрпризов, оплачивается из имеющегося кредита.

Естественно, на мобильный телефон можно будет также позвонить, независимо от страны, где он находится, набрав его номер в Швейцарии (в виде 00 41 79 36 XX XXX).

Голосовой почтовый ящик (который называется «ComBox») – это дополнительная услуга, управляемая дистанционно через USSD и доступная по прямому номеру (+41 86 079 36 XX XXX) до тех пор, пока она не дезактивирована. Разумеется, поступление голосового сообщения сигнализируется при помощи SMS.

Когда почтовый ящик не активирован, безуспешные звонки на мобильный телефон совершенно ничего не стоят.

На территории некоторых стран карта GSM CARD easyRoam, кроме того, дает доступ к сетям многочисленных конкурирующих операторов (см. раздел 6.2). Это обеспечивает непревзойденное качество обслуживания и максимальную безопасность, не говоря уже об определенной конфиденциальности.

С учетом срока действия кредитов на соединения (по крайней мере, один год вместо одного или двух месяцев) такое решение может представлять особый интерес для тех абонентов, которые пользуются мобильным телефоном время от времени, поскольку стоимость минуты все-таки достаточно высока, а поступающие (входящие) звонки должны оплачиваться.

Прием коротких сообщений, напротив, остается полностью бесплатным, тогда как применение SIM-инструментария кроме того позволяет бесплатно посылать их при помощи преобразования USSD (*122*92*NUMERO*TEXTE#).

За получением более подробной информации следует обратиться к инструкциям пользователя, содержащимся в виде PDF-файлов в каталоге ROAMING компакт-диска[1], или на сайт компании Swisscom. Если принять во внимание усложненную и все более и более критикуемую тарификацию, которая используется операторами при роуминге, подобные решения имеют все шансы для успешного развития. Страны с небольшим числом населения действительно располагают избыточным количеством телефонных номеров, особенно при использовании «открытой» телефонной нумерации (то есть с переменным числом цифр в номере).

[1] В целях снижения стоимости издания компакт-диск к книге не прилагается. Вы можете бесплатно загрузить все упоминаемые в книге программы с сайта издательства www.dmkpress.ru (примерный объем архива 60 Мб) или, если у вас нет доступа в Internet, заказать компакт-диск наложенным платежом.

3 МОБИЛЬНЫЙ ТЕЛЕФОН

Мобильный телефон стандарта GSM представляет собой промышленное изделие высокой сложности, объединяющее в своем очень небольшом по размеру корпусе множество самых современных электронных компонентов (см. рис. 3.1).

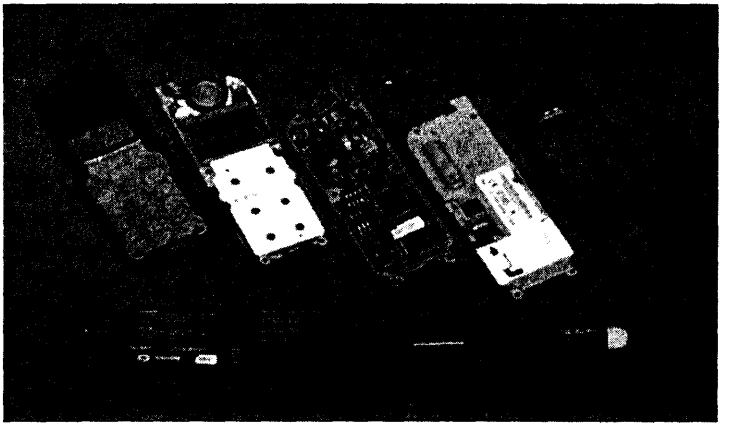


Рис. 3.1. Составные части мобильного телефона

Если бы была возможность приобрести некоторые из этих компонентов в розницу, то их цена в некоторых случаях была бы выше действительной продажной стоимости мобильного телефона. Вполне естественно, что это заставляет потребителя призадуматься по поводу реальной цены этих телефонов, которые иногда продаются дешевле, чем используемые в них аккумуляторные батареи или любой другой простой аксессуар[1].

Можно предположить, что телефон высшего класса должен выходить с завода по оптовой цене, составляющей несколько десятков евро. При этом он иногда перепродается за чисто символическую цену новому клиенту того или иного оператора, а торговые дилеры получают неплохую прибыль.

Чтобы речь не шла об убыточности продаж, следует ввести понятие стоимости приобретения абонента, в которую входят как рекламные

[1] Имеется в виду широко распространенная в западных странах практика, когда сотовые телефоны продаются операторами по очень низкой цене при условии заключения с клиентом контракта (абонемента) на обслуживание данного телефона. – *Прим. науч. ред.*

кампании, так и участие, иногда чрезмерное, в поставках мобильного телефона. И это еще не так дорого, если посмотреть на совершенно нереальную стоимость, по которой на рынке оценивается каждый абонент оператора.

Хорошо еще, если клиент окажется надежным, и будет месяц за месяцем возвращать вложенные в него инвестиции. Однако это предполагает приложение постоянных усилий по совершенствованию услуг, предлагаемых как своим абонентам, так и клиентам, которые предпочитают тарифные планы на основе предварительной оплаты и могут переходить от одного оператора к другому чуть ли не ежедневно, с очень малыми для себя затратами.

3.1. СТРОЕНИЕ МОБИЛЬНОГО ТЕЛЕФОНА СТАНДАРТА GSM

На рис. 3.2 представлена примерная структурная схема мобильного телефона GSM, условно разделенного на некоторое число функциональных блоков, которые не всегда соответствуют реальному распределению компонентов по печатным платам. Внешний вид печатной платы мобильного телефона приведен на рис. 3.3 и 3.4.

Прогресс технологий в области микроэлектроники приводит к повышению степени интеграции элементов и увеличению числа функций, выполняемых каждой интегральной схемой.

Вместе с тем на сегодняшний день для создания мобильного телефона высокого уровня производителям все еще требуется от 300 до 600 компонентов (активных и пассивных).

Радиоблок

Несмотря на то что радиоблок имеет очень важное значение, а его практическая реализация требует тщательного исполнения, все-таки он является не самой сложной частью мобильного телефона GSM. Этот блок совмещает функции передачи и приема, которые в значительной степени управляются блоком логики, и состоит в основном из малошумящих усилителей, фильтров, управляемых генераторов, а также схем модуляции и демодуляции.

Радиоблок должен максимально использовать возможности антенны, которая уменьшена до минимального размера и в скором времени превратится в компонент поверхностного монтажа на основной печатной плате. От него также требуется высокая эффективность использования энергии, чтобы обеспечить мобильному телефону работу в режиме передачи в течение нескольких часов при питании от аккумуляторной батареи средней емкости.

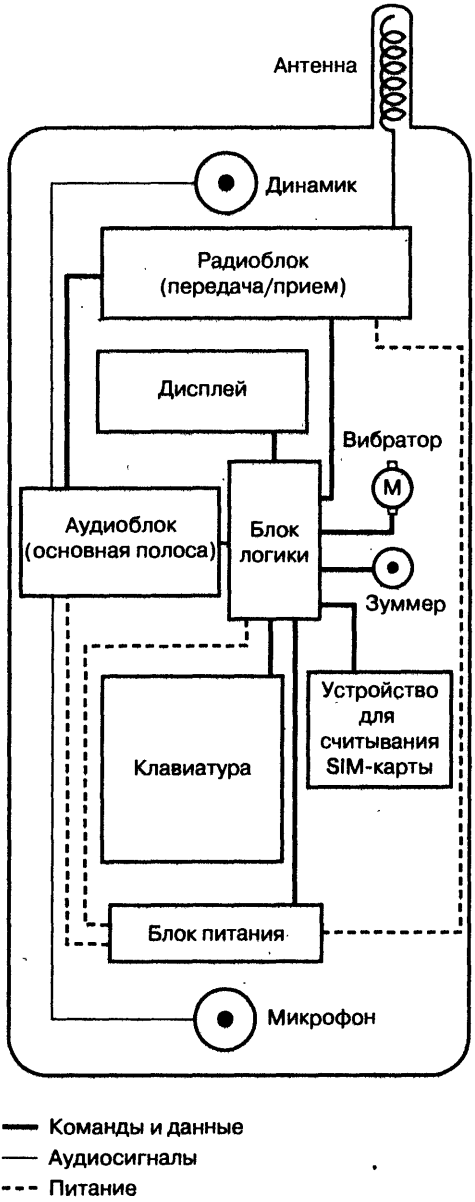


Рис. 3.2. Структурная схема мобильного телефона системы GSM

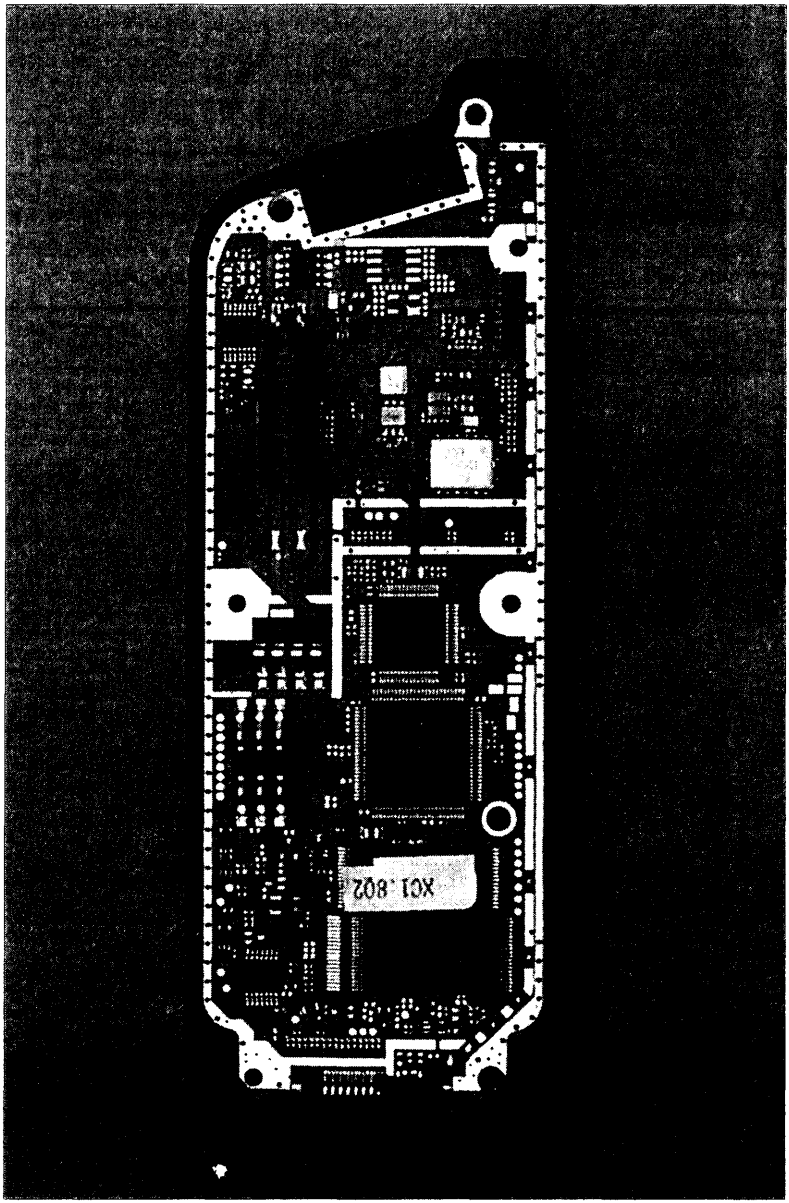


Рис. 3.3. Основная печатная плата мобильного телефона (вид сверху)

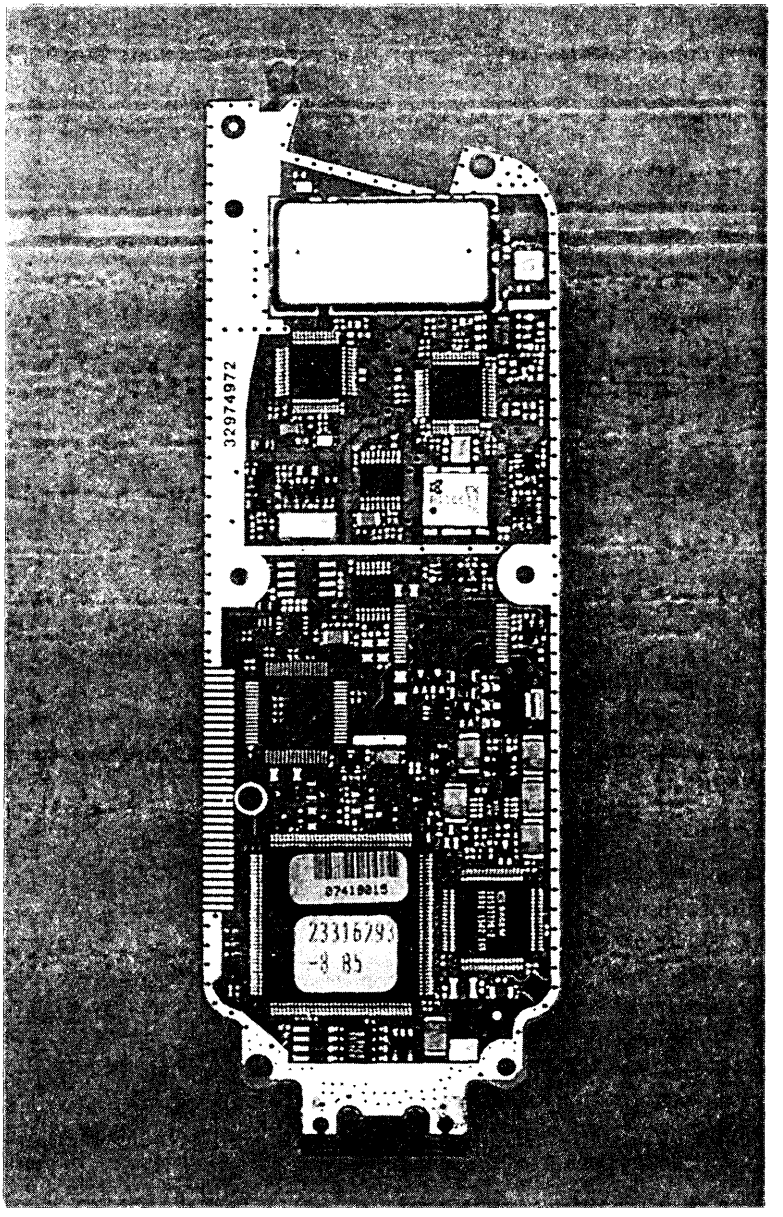


Рис. 3.4. Основная печатная плата мобильного телефона (вид снизу)

Передающий блок функционирует только во время телефонной связи: он передает короткие пакеты данных, когда мобильный переходит из одной соты в другую или когда по запросу сети периодически сообщает свое местоположение. То же самое происходит перед тем, как телефон зазвонит (поскольку сначала он подтверждает свое присутствие в сети), или при получении SMS-сообщения (когда он подтверждает, что сообщение получено).

Следовательно, необходимо учитывать, что мобильный телефон GSM может перейти в режим передачи в любой момент, поэтому его надо полностью отключать перед попаданием в ту зону, где его использование было бы нежелательным, а также во избежание постоянного отслеживания его перемещений со стороны сети.

Напомним, что если просто воздерживаться от звонков или ответов на них, а также отключить сигналы звонка, это ни в коем случае не является достаточной мерой безопасности.

Технические характеристики радиоблоков различных моделей значительно отличаются друг от друга. На территориях, имеющих недостаточное покрытие, некоторые мобильные телефоны могут работать устойчиво, а другие нет, даже если они обслуживаются одним и тем же оператором.

Иногда хороший показатель автономности работы телефона «компенсируется» меньшим радиусом его действия в сложных условиях, между тем в определенных многодиапазонных моделях мобильных телефонов могут до некоторой степени допускаться необходимые компромиссы, предполагаемые их концепцией.

На основной печатной плате радиоблок располагается как можно ближе к антенне и является объектом, в отношении которого предпринимаются строжайшие меры предосторожности с точки зрения электромагнитной совместимости. Это объясняется тем, что он находится всего в нескольких сантиметрах от схем, обладающих высокой чувствительностью, в то время как хорошо известно, что работающий мобильный телефон GSM может вызывать помехи в радиусе нескольких метров.

Аудиоблок

В состав аудиоблока, или блока обработки сигнала основной полосы, помимо собственно схем, обеспечивающих его работу, входят также микрофон и микротелефон, а если мобильный телефон оснащен комплектом типа hands free, то еще и динамик.

Одной из основных функций данного блока является кодирование и декодирование сигналов при помощи так называемого кодека,

иначе говоря, КОдера-ДЕКодера. Таким образом, к функциям аналого-цифрового и цифро-аналогового преобразования добавляются сжатие и декомпрессия данных, необходимые для получения хорошего качества звука при низкой скорости передачи данных.

При современном уровне техники этот блок практически всегда выполняется на базе цифрового процессора сигналов DSP, хорошо адаптированного к таким действиям в режиме реального времени. Большая мощность обработки сигнала позволяет внедрить такие «продвинутые» функции, как встроенный блок hands free или даже распознавание голоса.

Между аудио- и радиоблоками расположен квадратурный I/Q-модулятор, который преобразует передаваемые биты в изменение фазы на 90°, и соответствующий демодулятор, выполняющий обратное преобразование.

Разделение функций между блоками обработки сигнала «основной полосы» и «логикой» более размыто, поскольку последний оснащен микропроцессором, к семейству которого теоретически можно причислить и цифровой процессор сигналов. Поэтому за неимением одного единого процессора, осуществляющего все функции, вполне можно доверить несколько чисто логических задач процессору сигналов, если у него остается некоторое свободное время, или, наоборот, передать на выполнение небольшую часть обработки сигнала основному микропроцессору.

Блок логики

Основной микропроцессор, который является настоящим «сердцем» мобильного телефона, выполняет чрезвычайно сложные логические операции, запрограммированные в памяти, которую можно обновлять дистанционно. Именно в программе микропроцессора заложены все функциональные особенности аппарата, начиная с системы меню.

Помимо клавиатуры и дисплея (определяемых, согласно стандарту GSM, как интерфейс «человек-машина») блок логики управляет зуммером, выполняющим роль звонка, устройством вибрации, блоками аудио и радио (синтезатором частот), устройством для считывания SIM-карт и даже устройством для заряда батарей.

Добавим к этому списку «периферийных устройств» энергонезависимую защищенную память, в которой записаны «конфиденциальные» данные, такие как коды «отпирания» или идентификационный номер (IMEI) мобильного телефона.

Подключение к определенным контактам универсального соединительного разъема телефона позволяет техническим специалистам

вести «диалог» с микропроцессором при помощи соответствующего терминала и осуществлять таким образом множество операций, обычно недоступных конечному пользователю.

Тем не менее в Internet можно найти информацию для той или иной конкретной модели мобильного телефона, позволяющую экспериментировать с этой мощной, но небезопасной функцией.

SIM-карта

SIM-карта – настоящий ключ идентификации и аутентификации владельца мобильного телефона. Она устанавливается в специальное соединительное устройство, связанное с блоком логики при помощи соответствующих схем сопряжения.

SIM-карта (см. рис. 3.5) – это асинхронная чип-карта, соответствующая одновременно спецификациям и стандарта ISO 7816, и стандарта GSM 11.11.

Для читателей, знакомых с чип-картами, отметим, что SIM-карта работает согласно протоколу T = 0, а ее классом ISO является класс A0h.

Если SIM-карту вынуть из мобильного телефона, то ее можно вставить в любое устройство для считывания чип-карт, использующих данный протокол. При этом надо будет склеить кусочки карты с помощью клейкой ленты, если телефон использует карту микроформата, полученную из карты размера ISO, предварительно разрезанную в соответствии с рис. 3.6.

Рис. 3.5. Внешний вид SIM-карты, которая является обычной чип-картой ISO 7816

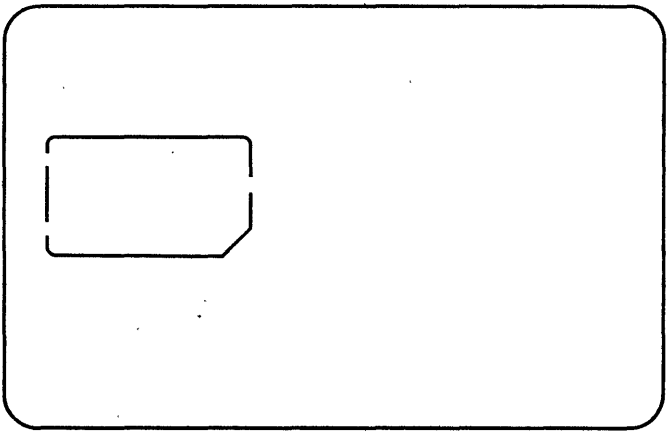


Рис. 3.6. Вырезание микро SIM-карты из карты размера ISO

Таким образом, устройство для считывания чип-карт, соединенное с совместимым компьютером, предоставляет возможность вести считывание и запись любой SIM-карты при помощи либо программы общего характера (обычная передача команд ISO), либо специализированной. Ниже приведен стандартизированный набор команд, признаваемый всеми SIM-картами, который позволяет выполнять множество операций, при условии, что логическое строение карты хорошо известно:

20h: проверить CHV;
24h: изменить CHV;
26h: дезактивировать CHV;
28h: активировать CHV;
C0h: получить ответ;
32h: увеличить;
04h: объявлять недействительным;
B0h: считывать двоичный код;
B2h: считывать запись;
44h: восстановить;
88h: запустить алгоритм GSM;
A2h: поиск;
A4h: выбор;
FAh: режим ожидания;
F2h: состояние;
2Ch: разблокировать CHV;
D6h: обновить двоичный код;
DCh: обновить запись;
10h: профиль терминала;
C2h: конверт;

12h: выборка;
14h: ответ терминала.

Глава 5 данной книги полностью посвящена этому аспекту исследования мобильных телефонов GSM.

На данный момент ограничимся лишь указанием на то, что SIM-карта содержит мощный микропроцессор, способный при помощи соответствующих команд вести диалог с микропроцессором телефона, и память с более чем значительным объемом 8–32 Кб для современных поколений мобильных телефонов (фазы 2 и 2+). А такие производители, как Gemplus, уже сейчас готовят будущие поколения карт.

Помимо объема памяти не менее важна и мощность операционной системы карты (иначе говоря, содержащейся в ней логики).

Процессор SIM-карты практически начинает конкурировать с процессором телефона, уже не ограничиваясь только управлением доступа к данным, содержащимся на карте, и выполнением криптографических алгоритмов. Осуществляется также включение собственных, помимо исходных, меню (технология SIM Toolkit), управляющих мобильным телефоном (Proactive SIM), или непосредственное выполнение дополнительных приложений, таких как, например, мини-навигатор Internet или «электронный кошелек».

Последующие поколения мобильных телефонов, вне всякого сомнения, будут относиться к типу dual-slot (с двойным разъемом). При этом второе считывающее устройство будет позволять наряду с SIM-картой работать, например, с банковскими картами.

Блок питания

На сегодняшний день в мобильных телефонах используются никель-кадмиевые (Ni-Cd), никель-металлогидридные (Ni-MH) или литиево-ионные (Li-ion) аккумуляторные батареи.

Новейшие достижения не только в области источников питания мобильных телефонов, но и технологии исполнения аккумуляторных батарей и устройств для их зарядки (эти вопросы были рассмотрены в моей книге «Alimentations a piles et accus») обеспечивают более чем достаточный уровень автономной работы.

Остается только отметить, что некоторые производители предпочитают сохранить возможность питания телефона от «одноразовых» батареек, что может оказаться весьма полезным в неотложных ситуациях. Комплект новых алкалиновых батареек в действительности обеспечивает значительно более длительную работу мобильного телефона в автономном режиме, чем полностью заряженный аккумулятор. Срок

хранения данных батареек составляет несколько лет, в отличие от нескольких десятков дней, по истечении которых аккумуляторная батарея начинает самостоятельно разряжаться даже (и особенно), если она все это время не работала.

Основная роль блока питания – обеспечить различные схемы мобильного телефона требуемыми для их работы точными величинами напряжений до полного истощения аккумуляторной батареи.

Поэтому часто этот блок содержит несколько стабилизаторов напряжения: либо линейных – с низким падением напряжения (LDO – Low DropOut), либо импульсных.

Как правило, мобильный телефон оснащен аккумуляторной батареей 3,6 В (то есть тремя элементами по 1,2 В), при помощи которой обеспечивается питание мощных каскадов радиоблока напряжением 3,0 В, остальной части радиоблока – напряжением 2,8 В и схем обработки сигналов основной полосы – напряжением 2,0 В.

Блок логики и SIM-карта, в свою очередь, обычно питаются напряжением 3 В или, в случае использования импульсного повышающего трансформатора, – напряжением 5 В.

Другая функция блока питания состоит в управлении аккумуляторной батареей. Чаще всего это оказываются схемы заряда (собственно «зарядное устройство» представляет собой простой источник питания, более или менее стабилизированный), а также схемы, необходимые для постоянной индикации состояния разряда/заряда батареи.

Такой «измеритель заряда» (gas gauge) может быть более или менее усовершенствованным, но в любом случае он важен для пользователя. Аккумулятор, находящийся в состоянии, близком к полному разряду, «предупреждает» об этом значительно раньше, чем батарейка.

В лучшем случае система заряда ведет точный учет потребления напряжения питания, а также числа полных или частичных перезарядов. Иногда она может даже обеспечивать последовательное подключение нескольких аккумуляторных батарей, используемых по очереди.

Поэтому определенные батареи имеют специальный номер, записанный в постоянной памяти, что, в частности, усложняет использование других аккумуляторов вместо предлагаемых (по высокой цене) производителем.

Специальные зарядные устройства показаны на рис. 3.7 и 3.8.

Антенны

В мобильном телефоне применяется четвертьволновая «штыревая» антенна. Для используемых частот длина антенны составляет

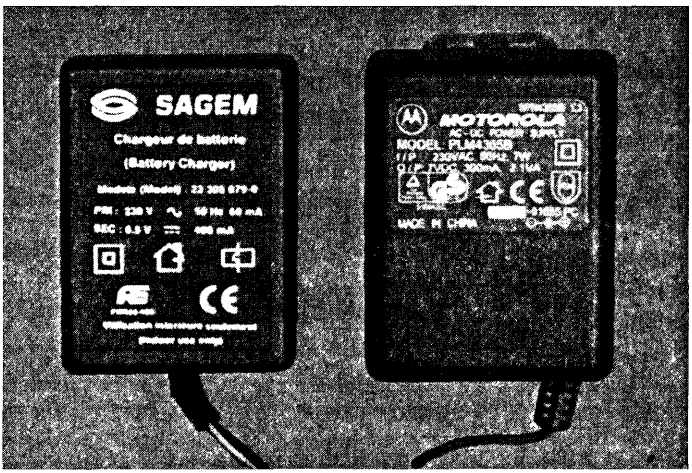


Рис. 3.7. Внешний вид двух специальных зарядных устройств (стабилизированные источники питания)

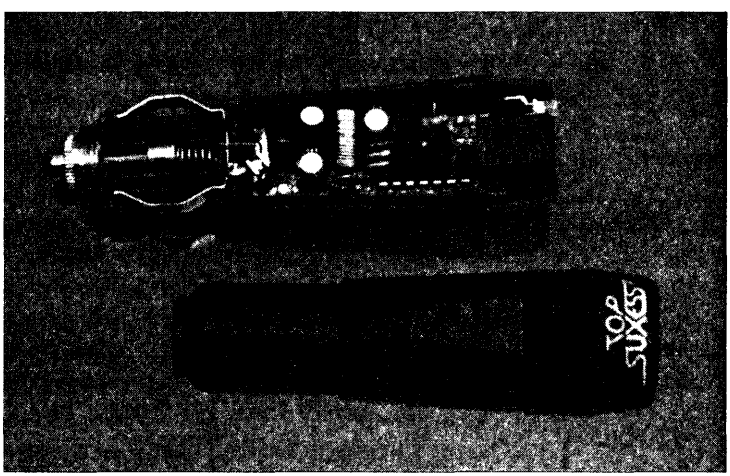


Рис. 3.8. Внутренний вид импульсного прикуривателя

приблизительно 8 см для GSM 900 и 4 см для GSM 1800, что соответствует варианту, показанному на рис. 3.9.

На этом рисунке указана длина антенны, которая практически равна длине выдвижных антенн, применявшихся ранее в некоторых моделях мобильных телефонов. Антенна такого типа обладает хорошей

эффективностью, а ее длина подобрана таким образом, чтобы свести к минимуму уровень облучения головы пользователя. Остается только ждать, чтобы большинство клиентов начали требовать еще более коротких антенн или вообще их отсутствия. Поэтому производители с готовностью взялись за изготовление четвертьволновых антенн уменьшенного размера, «спиральная» технология которых несколько напоминает антенны CB[1], созданные для приведения обычной четвертьволновой штыревой антенны длиной 2,6 м к приемлемому размеру. Иными словами, антенна представляет собой четвертьволновый провод в форме пружины (выполняя при этом роль дросселя), заформованный в пластик или каучук, как показано на рис. 3.10.

Рис. 3.9. «Штыревая» четвертьволновая антенна для GSM 900

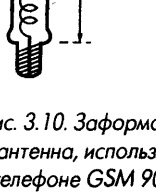


Рис. 3.10. Заформованная антенна, используемая в телефоне GSM 900/1800

В действительности внутри телефона остается короткий прямолинейный участок антенны, а ее внешняя (и заменяемая) часть практически не превышает 2–3 см в длину для диапазона 900 или 1800 МГц.

Поскольку некоторые клиенты к тому же считают такой тип антенны слишком неудобным (или ломким и даже опасным), все чаще применяются сверхминиатюрные антенны, которые припаиваются непосредственно к печатной плате. Таким образом, самые миниатюрные мобильные телефоны могут обойтись без наружной антенны, причем их характеристики в радиодиапазоне остаются вполне приемлемыми.

В конце концов, скоро четвертьволновые антенны, даже уменьшенные в размере, можно будет встретить практически только на крышах автомобилей.

Тем не менее стоит уточнить, что при увеличении указанной длины антенны повышается ее эффективность. Например, оснащение автомобиля антенной GSM типа «5/8» (приблизительно 20 см) создаст дополнительные преимущества.

---

[1] Citizen radio Band – диапазон, выделенный для персональной и служебной радиосвязи. – *Прим. науч. ред.*

Полуволновый вибратор, обладающий длиной, равной удвоенной длине четвертьволновой штыревой антенны, заменяет второй четвертьволновый участок «заземления», образованный электрическим корпусом телефона и телом пользователя. Это приводит к конфигурации, показанной на рис. 3.11, и, следовательно, к длине антенны, составляющей приблизительно 16 см.

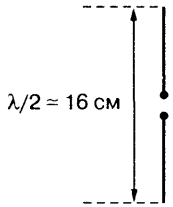


Рис. 3.11. Полуволновый вибратор телефона GSM 900

Большая часть антенн базовых станций оснащена излучающими элементами именно такого типа, имеющими поперечную поляризацию (кросс-поляризацию). Продуманное сочетание множества вибраторов позволяет изменять направленность действия антенн в соответствии с необходимыми условиями.

Теоретически можно пойти еще дальше по этому пути и использовать в телефонах GSM антенны типа «волновой канал», аналогичные антеннам, применяемым в телевидении для приема сигналов диапазона ДМВ (см. рис. 3.12). Значительное усиление, полученное таким образом в выбранном направлении излучения, позволило бы использовать мобильные телефоны в некоторых зонах, находящихся на границе охвата радиорелейными станциями. Такие антенны начинают

Рис. 3.12. Антенна типа «волновой канал» может совершать настоящие чудеса

появляться в продаже, однако их можно изготовить самостоятельно, причем это обойдется вам гораздо дешевле.

Вибраторы

Вибратор, которым оснащено большинство мобильных телефонов, заменяет звонок в тех случаях, когда требуется известная конфиденциальность. Поскольку он практически бесшумен, необходимо, чтобы пользователь носил телефон при себе.

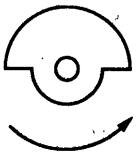


Рис. 3.13. Вид эксцентрика вибратора в разрезе

Хотя это и кажется несколько анахроничным в среде высоких технологий мобильных телефонов, но многие вибраторы работают полностью на электромеханическом принципе. Микродвигатель постоянного тока заставляет вращаться с довольно высокой скоростью элемент типа эксцентрика, в большинстве случаев имеющий форму, приведенную на рис. 3.13. Внешний вид микродвигателя и эксцентрика вибратора показан на рис. 3.14.

Вращение подобной, явно несбалансированной и довольно массивной детали, естественно, порождает сильную вибрацию, бесшумную, но хорошо ощутимую.

Механический принцип используется и во многих автономных вибраторах, которые предназначены для мобильных телефонов, не

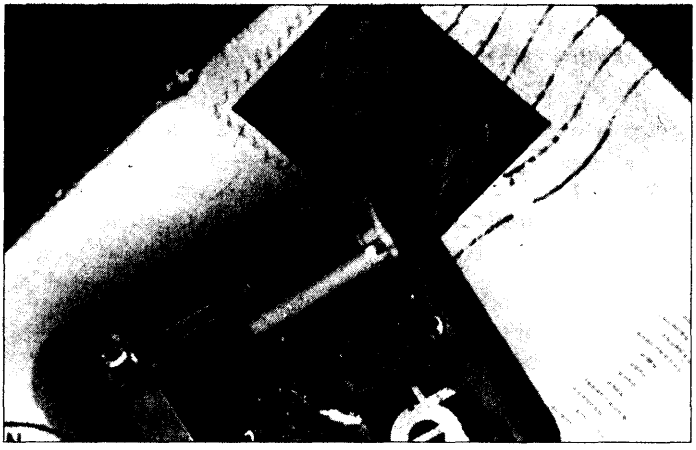


Рис. 3.14. Внешний вид микродвигателя и эксцентрика вибратора

оснащенных ими изначально. Вибраторы включаются по реакции мобильного телефона в ответ на запрос, поступивший от сети на имеющийся вызов.

Необходимо учитывать, что такие вибраторы потребляют значительно больше электрической энергии, чем звуковые устройства. При этом потребление тока обычно составляет более 100 мА, поэтому следует иметь в виду, что излишне частое использование вибратора может существенно снизить автономность работы аккумуляторной батареи.

3.2. ОСНОВНЫЕ ТИПЫ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Прогресс в области мобильных телефонов идет с еще большей скоростью, чем в области компьютеров. Новый мобильный телефон может оказаться устаревшим уже через неделю после покупки.

Конечно, наибольшее впечатление производят новинки, позволяющие использовать мобильные телефоны в сети Internet, хотя многие клиенты продолжают покупать мобильные только для того, чтобы просто иметь возможность позвонить.

Аппараты, считающиеся уже устаревшими, вполне способны превосходно выполнять такие основные функции, как голосовая связь и прием коротких сообщений, причем часто с отличным качеством.

Важной составляющей эволюции является миниатюризация, которая, в конце концов, может привести к появлению мобильных телефонов размером с наручные часы, хотя, с другой стороны, основная тенденция состоит в увеличении размеров дисплеев и «расширении» клавиатуры.

Схемам, которые ранее получали питание от батареи, состоящей из четырех элементов по 1,2 В (то есть 4,8 В), на сегодняшний день часто бывает достаточно и напряжения 3,6 В (всего трех элементов), если не меньше.

С точки зрения функционирования необходимо различать одно-, двух- и даже трехдиапазонные мобильные телефоны (900, 1800 и 1900 МГц).

Учитывая более высокие объемы производства, а также экономические и технические факторы, можно с уверенностью предположить, что в скором времени будут производиться только многодиапазонные мобильные телефоны.

Практически все они будут предназначены также для работы в режиме кодировки звука EFR, который отныне поддерживают все соты всех сетей.

Что касается «третьего поколения» мобильной связи, то переход к UMTS, по-видимому, будет происходить на базе GPRS, поскольку технология WAP не смогла привлечь пользователей. Кроме того, потребителям должны быть представлены достаточно убедительные предложения и за приемлемую плату. Ведь пользователи не слишком-то будут стремиться к переходу, если основной идеей при этом будет плата (и большая) за то, что они привыкли получать бесплатно. Хотя, в конечном счете, именно этот принцип лежит в основе успехов компании MINITEL.

«Персонализированные» мобильные телефоны

Наряду с чисто техническими моментами, которые были рассмотрены выше, необходимо знать, что мобильные телефоны, «субсидированные» операторами, могут иметь некоторые особенности. Они необязательно бывают столь явными, как название торговой марки, стоящей на корпусе или появляющейся на дисплее в качестве приветственного послания, не говоря уже о более или менее запоминающихся мелодиях звонка.

Помимо закрепления за своей собственной сетью или службой, речь о которой пойдет ниже, некоторые операторы предлагают мобильные телефоны, лишенные каких-либо дополнительных с точки зрения спецификации GSM функций. И, как ни странно, если кто-нибудь решит перейти к другому оператору, то катастрофически не хватать будет именно их.

Например, при наличии международной карты с предварительной оплатой мобильный телефон, который не поддерживает функции нестандартной дополнительной услуги USSD, предоставляет возможность только принимать звонки и короткие сообщения, но при этом нельзя звонить ни по каким другим номерам, кроме номера срочной помощи и невозможно узнать о размере оставшегося кредита.

Мобильные терминалы GPS

Немало сложных, но популярных электронных функций отныне стали доступны в форме модулей, которые могут рассматриваться в качестве простых составных частей. Примером тому служат приемники системы позиционирования при помощи спутников GPS (Global Positioning System – глобальная система навигации и определения местоположения), одновременно с этим являющиеся мобильными телефонами стандарта GSM.

Модуль терминала GPS представляет собой устройство, помещенное в тщательно экранированный корпус, которое готово к связи с внешним миром после подсоединения нескольких элементов: источника питания, антенны, телефонной трубки или системы hands free и даже компьютера (интерфейс RS-232). Такие модули, часто имеющие выходную мощность 8 Вт, нередко можно встретить в телефонных установках на автомобилях или кораблях, где они иногда совмещены с системой навигации или оповещения.

В промышленной сфере их используют в системах дистанционного управления или телеметрии на изолированных участках местности (насосных станциях, при проведении анализа степени загрязнения окружающей среды и т.д.), а также для оказания помощи, в случае надобности, жизненно важным «проводным» линиям.

Помимо этого такие устройства применяют в сочетании со схемами интерфейса для классического телефонного оборудования, чтобы обслуживать абонентов, недоступных по «проводной» линии связи, или для предоставления возможности через частный автокоммутатор позвонить при помощи сети GSM абоненту мобильной связи с минимальными затратами.

Внутренний вид модуля мобильного терминала GPS мощностью 8 Вт приведен на рис. 3.15 и 3.16.

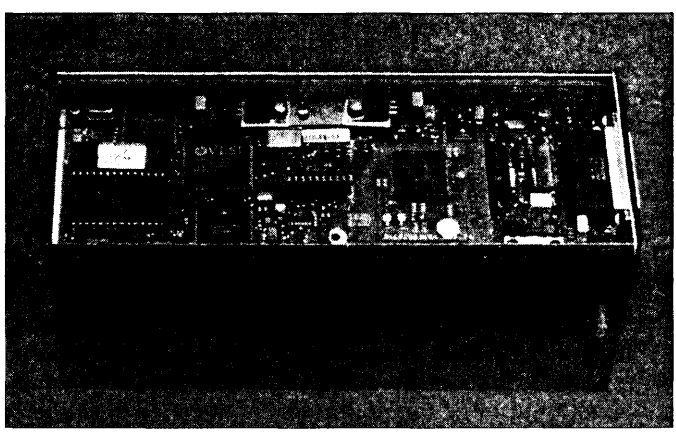


Рис. 3.15. Внутренний вид модуля мобильного терминала GPS мощностью 8 Вт

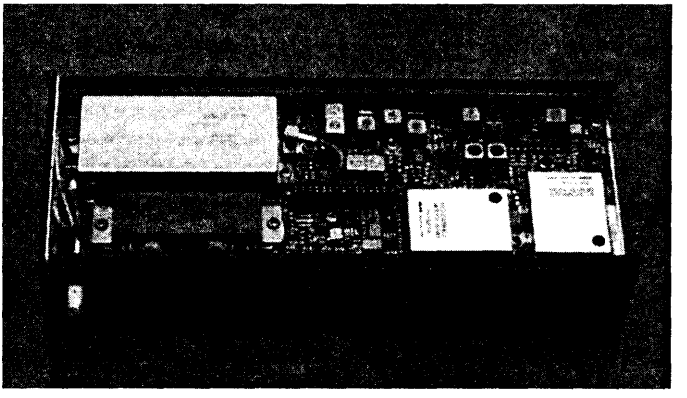


Рис. 3.16. Внутренний вид модуля мобильного терминала GPS мощностью 8 Вт

3.3. ИНТЕРФЕЙС ПОЛЬЗОВАТЕЛЯ

То, что в спецификации GSM носит название интерфейса «человек-машина», объединяет в себе все, что позволяет пользователю вести диалог с операционной системой мобильного телефона.

Помимо клавиатуры и дисплея (который может быть текстовым или графическим, монохромным или цветным) к интерфейсу пользователя следует также отнести устройство звонка и динамик (или громкоговоритель) с функциями воспроизведения тональных сигналов (или мелодий) вызова. Очень часто подобное воспроизведение осуществляется не сетью, а мобильным телефоном по ее команде. Это позволяет при существенной экономии передающих ресурсов гарантировать пользователю воспроизведение поступающих в данный момент тональных сигналов звонка, даже если сеть не в состоянии довести их до него.

Тональности сигнализации

Тональности, обычно использующиеся для сигналов вызова, имеют высоту, соответствующую частоте 425 Гц (с допуском 15 Гц), которая в принципе мало чем отличается от частоты 440 Гц (нота «ля») «проводной» телефонной связи.

Основное отличие заключается в том, что отсутствует сигнал (тон) приглашения к набору номера: набирать номер (или искать его в записной книжке) всегда начинают, еще не зная, сможет ли сеть обеспечить прохождение вызова.

Нажатие на кнопку подтверждения (как правило, зеленого цвета) отправляет сети запрос на вызов в виде пакета битов. Таким образом, тональные сигналы типа DTMF (двухтонального многочастотного набора), которые обычно слышны в динамике телефона во время набора номера, служат только для заполнения паузы и никуда не передаются.

В качестве дополнения может быть предусмотрен звуковой сигнал частотой 425 Гц и длительностью 200 мс, сообщающий пользователю о том, что вызов принят.

В случае перенасыщения сети появляется тот же самый тон, но повторяемый с интервалами 200 мс, иначе говоря, быстрее, чем в случае, когда занят номер вызываемого абонента (500 мс через каждые 500 мс).

Если радиоканал недоступен, то прозвучат три звуковых сигнала по 200 мс с интервалами по 200 мс.

Та же частота 425 Гц используется для сигнализации «обратного вызова» (имитирующего звуковой сигнал вызываемого телефона, синхронность при этом, однако, не гарантируется) и для оповещения о вызовах, ждущих своей очереди (звуковой сигнал длительностью 200 мс, пауза 600 мс, звуковой сигнал 200 мс, пауза 3 с и т.д.).

Более специфичные ситуации (запрещенный номер или невозможность аутентификации и т.д.) обозначаются тремя последовательными тональными сигналами 950, 1400 и 1800 Гц. Запись этих сигналов представлена в каталоге SONS на компакт-диске. В некоторых случаях в качестве подтверждения диагностики на дисплее телефона может появиться текст.

Обычные команды

Доступ ко многим функциям телефона и сети можно получить с помощью системы меню, организация которого значительно отличается в разных моделях мобильных телефонов.

Но тех же результатов можно достичь путем простого набора на клавиатуре телефона специальных кодов, о которых руководства по пользованию предпочитают умалчивать. Такой способ действия часто дает доступ к функциям, которые отсутствуют в меню и даже не задокументированы. Некоторые из таких кодов относятся к определенной модели или марке мобильного телефона, хотя большинство из них стандартизированы.

Самым популярным кодом, вне всякого сомнения, является код *#06#, с помощью которого можно раскрыть международный идентификационный номер (IMEI) мобильного телефона, служащий, в частности, основой для вычисления возможного кода «отпирания»

телефона. Декодирование этого номера, являющегося уникальным и состоящим из 14 цифр плюс ключ контроля, не лишено определенного интереса. В качестве примера можно рассмотреть международный номер (вымышленный) телефона «МСТ» (персонализированный вариант RC712 SAGEM):

330072350123451

Две первые цифры (0072) указывают на страну происхождения мобильного телефона согласно международному коду нумерации телефонной связи. В данном примере цифры 33 обозначают Францию.

Четыре последующие цифры являются кодом подтверждения типа TAC (Type Approval Code), идентифицирующим модель телефона по отношению к процедуре соответствия.

Идущие следом две цифры (35) представляют собой код окончательной сборки FAC (Final Assembly Code), который уточняет место сборки телефонного аппарата. Может быть, это простое совпадение, но в Бретани (35-й департамент) действительно есть заводы, где производятся мобильные телефоны.

Последующие шесть цифр (в данном случае намеренно сведенные к 012345) являются серийным номером (SNR) телефона рассматриваемой модели.

И наконец, замыкающая цифра представляет собой «ключ Luhn»[1], который вычисляется таким же образом, как и последняя цифра номеров банковских карт, SIREN и т.п.

Небольшая программа IMEI.BAS (см. каталог BASIC на компакт-диске) позволяет быстро проверить данный международный идентификационный номер IMEI (включающий ключ и состоящий, таким образом, из 15 цифр).

```
10 REM ----- IMEI.BAS -----
20 KEY OFF:CLS
30 CLEAR:PRINT:PRINT"Ввести номер IMEI":INPUT N$
40 L=LEN(N$):DIM N(L)
50 FOR F=1 TO L
60 C$=MID$(N$,F,1):C=VAL(C$):N(F)=C
70 NEXT F
80 IF (L/2)-INT(L/2)=0 THEN 170
90 T=0:FOR F=2 TO L-1 STEP 2
```

[1] Подробнее об этом см. в книге этого же автора «Магнитные карты и ПК», М.: ДМК Пресс, 2001. – *Прим. науч. ред.*

```
100 C=2*N(F):IF C>=10 THEN C=C-9
110 T=T+C:NEXT F
120 FOR F=1 TO L STEP 2
130 T=T+N(F):NEXT F
140 IF T>=10 THEN T=T-10:GOTO 140
150 IF T=0 THEN PRINT"IMEI подтвержден":GOTO 30
160 PRINT"IMEI не подтвержден":GOTO 30
170 T=0:FOR F=1 TO L-1 STEP 2
180 C=2*N(F):IF C>=10 THEN C=C-9
190 T=T+C:NEXT F
200 FOR F=2 TO L STEP 2
210 T=T+N(F):NEXT F
220 GOTO 140
230 REM (c)1996,2000 Patrick GUEULLE
```

Конечно, этот простой арифметический тест ни в коей мере не подтверждает аутентичности номера, а просто говорит о его правдоподобности.

Рассмотрим еще один пример – международный номер IMEI мобильного телефона марки Motorola M3188:

448836080123455

Он представляет интерес с той точки зрения, что позволяет развеять всяческие сомнения по поводу маркировки «made in UK», стоящей на самом телефоне, и «made in Germany» – на упаковке (не говоря уже о «made in China» на зарядном устройстве). Наконец, рассмотрим в качестве примера вымышленный идентификационный номер телефона, выпущенного фирмой Alcatel:

330045530123450

В Internet можно найти официальные программы, позволяющие вычислить коды «отпирания» (раскодирования) некоторых мобильных телефонов этой марки. В данном случае в результате выполнения такой программы был получен код 90442A50.

К полученному коду «конструктора» следует еще добавить шестнадцатеричное значение, характерное для каждого оператора. Для приведенного примера действует значение 009FDFFA (испанский оператор), в то время как использование значения 01BFDFF4 иногда приводит к неплохим результатам в случае французского оператора. Последний вариант можно предоставить для самостоятельного изучения читателям под их личную ответственность.

Абсолютно к другому типу относится код 10#, который активирует, например, вызов номера, стоящего на десятой позиции в телефонной книжке (функция ускоренного набора номера). При этом в зависимости от модели телефона может потребоваться или не потребоваться подтвердить операцию нажатием на кнопку зеленого цвета. Само существование этой стандартизованной команды вызывает серьезные сомнения по поводу утверждения, то представляемого в качестве совершенно официального предупреждения, то опровергаемого, согласно которому код 90# оказывает серьезную помощь пиратам. Этот абсолютно реальный код практически может только вызвать 90-й по порядку номер из записной книжки в режиме «двойного вызова», если он набран во время соединения..

Всегда следует помнить об очень полезных командах, позволяющих разблокировать SIM-карту после трех неудачных попыток введения кода персонального идентификационного номера PIN:

- **05*PUK*PIN*PIN# для PIN 1;
- **052*PUK*PIN*PIN# для PIN 2.

В обоих случаях PUK представляет собой код разблокирования, предоставляемый оператором и меняющийся в зависимости от того, надо ли разблокировать PIN1 или PIN2.

Специальные команды

В стандарте GSM оговаривается определенное число дополнительных услуг, которые могут предоставляться или не предоставляться операторами, а также включаться или не включаться в меню телефонов. Этими услугами можно управлять посредством специальных команд, структура которых остается неизменной:

```
Установка услуги: **SC*SI#
Активирование услуги: *SC*SI#
Дезактивация услуги: #SC*SI#
Запрос услуги: *#SC*SI#
Аннулирование услуги: ##SC*SI#
```

Код услуги SC (Service Code) определяет дополнительную услугу, к которой относится команда, а дополнительная информация SI (Supplementary Information) служит для передачи конфиденциального кода, если он есть, а также параметров, уточняющих производимое действие (например, на какой номер телефона следует переадресовывать вызовы).

Если в разграничивающей звездочке нет необходимости, она, соответственно, убирается, например, команда аннулирования принимает вид ##SC#. И наоборот, несколько звездочек могут разделять различные поля параметров, например, *SI становится *SIA*SIB*SIC*. Можно заметить, что такой синтаксис несколько напоминает синтаксис услуг Class проводных телефонов и даже цифровой сети с интеграцией услуг ISDN.

Ниже приведены основные дополнительные услуги, список которых, безусловно, будет только расти:

SC = 75: Услуга расширенного многоуровневого приоритета и прерывания обслуживания eMLPP (enhanced Multi Level Precedence and Preemption)
SC = 66: Переадресация вызова CD (Call Diversion)
SC = 30: Индикация идентификационного номера вызывающей линии CLIP (Calling Line Identification Presentation)
SC = 31: Ограничение идентификационного номера вызывающей линии CLIR (Calling Line Identification Restriction)
SC = 76: Индикация идентификационного номера подсоединенной линии COLP (COnnected Line Identification Presentation)
SC = 77: Ограничение идентификационного номера подсоединенной линии COLR (COnnected Line Identification Restriction)
SC = 21: Безусловная переадресация входящего вызова на другой номер CFU (Call Forwarding Unconditional)
SC = 67: Переадресация вызова, если номер занят CF Busy
SC = 61: Переадресация вызова в отсутствие ответа CF No Reply
SC = 62: Переадресация вызова в случае недоступности CF Not Reachable
SC = 002: Переадресация всех вызовов
SC = 004: Условная переадресация всех вызовов
SC = 43: Ожидание (двойной вызов) WAIT
SC = 361: Сигнал от пользователя пользователю UUS Service 1 (User to User Signaling)
SC = 362: UUS Service 2
SC = 363: UUS Service 3
SC = 360: все UUS
SC = 33: Запрещение всех исходящих звонков BAOC (Barring of All Outgoing Calls)
SC = 331: Запрещение всех исходящих международных звонков BAOIC (Barring of All Outgoing International Calls)
SC = 332: BAOIC, кроме страны происхождения
SC = 35: Запрещение всех входящих звонков BAIC
SC = 351: BAIC roaming
SC = 330: Запрещение всех звонков
SC = 333: Запрещение исходящих звонков

SC = 353: Запрещение входящих звонков
SC = 96: Явная (определенная) переадресация (передача) вызова ECT (Explicit Call Transfer)
SC = 37: Дозвон по занятому номеру CCBS (Completion of Calls to Busy Subscriber)
SC = 37: Дозвон по номеру, который не отвечает CCNRy (Completion of Calls to No Reply)
SC = 07n: SPNP (где n = 0 - 9)
SC = 59n: MSP (где n = 0 - 9)

Самые популярные из этих услуг касаются индикации номера звонящего, двойного вызова и особенно переадресации вызовов (в том числе на систему передачи голосовых сообщений) в самых разных ситуациях.

Несмотря на то что прослушивание автоответчика бесплатно, он является столь явным источником доходов для операторов, что они практически всегда активируют эту услугу по умолчанию и не поощряют своих клиентов ее дезактивировать.

Следует напомнить, что если автоответчик «доступного» телефона отключен, то мобильный телефон будет звонить столько времени, сколько необходимо для того, чтобы спокойно ответить на звонок (в частности, находясь за рулем автомобиля). Помимо этого за вызов, оставшийся без ответа, не нужно платить.

Когда мобильный телефон недоступен (отключен или находится вне зоны обслуживания), то голосовое сообщение «абонент недоступен» передается также совершенно бесплатно.

В этом случае достаточно перезвонить позже, как если бы номер был занят.

Некоторые формы абонемента позволяют неоднократно отключать автоответчик с помощью команды ##002#, однако обратное его включение может оказаться значительно сложнее. Для этого надо точно знать, на какой номер (специальный) должна быть запрограммирована переадресация.

Поэтому, прежде чем выполнить какое-либо окончательное действие, рекомендуется внимательно записать этот номер, который можно узнать, набрав, например, *#62# (запрос переадресации в случае недоступности).

Включение автоответчика в любом случае подразумевает уточнение, в каких случаях должна осуществляться переадресация и для каких типов звонков. Это выполняется при помощи кода группы

основных услуг BS (Basic Service Group), стоящего после назначаемого номера переадресации:

- 10 – все типы звонков;
- 11 – голосовые сообщения;
- 12 – данные;
- 13 – факсимильные сообщения;
- 16 – короткие сообщения (SMS);
- 19 – все звонки, кроме SMS-сообщений;
- 17 – группа голосовых услуг.

Можно только сожалеть о том, что в зависимости от оператора при использовании схемы с предварительной оплатой автоответчик нельзя ни отключить, ни даже изменить его функции при помощи клавиатуры (для этого необходимо обратиться в довольно дорогостоящую службу обслуживания клиентов Service Clients), а может случиться, что его нельзя будет отключить в принципе. Это еще раз подтверждает тот факт, что клиенты, пользующиеся тарифными схемами с предварительной оплатой, могут обслуживаться информационной системой, совершенно отличной от той, что обслуживает абонентов.

Тем не менее все эти схемы находятся в постоянном развитии, и услуги, которые не предоставлялись в них изначально, теперь уже стали их неотъемлемой частью.

В некоторых случаях клиентам может потребоваться отправить специальную команду, чтобы воспользоваться услугами.

Например, можно набрать *43# – чтобы активировать услугу двойного вызова «старой» карты с предварительной оплатой (в том случае, если мобильный телефон поддерживает соответствующую функцию), #43# – чтобы дезактивировать эту услугу, или *#43# – чтобы узнать, активна она или нет.

Случай запрещения звонков более сложен, поскольку при этом требуется задействовать пароль. Это относится, по крайней мере, к тем типам звонков, которые пользователь хочет заблокировать сам, так как совершенно очевидно, что блокировка, установленная оператором, может изменяться только им самим.

Например, речь может идти о международных звонках, сделанных с помощью той или иной национальной карты с предварительной оплатой, или непосредственно о любом прямом наборе номеров

с международной картой предварительной оплаты, работающей в режиме обратного вызова (call-back).

Вместе с тем можно провести последовательное тестирование сети за сетью, и даже соты за сотой, чтобы проверить, действует ли блокировка повсюду. Здесь вас вполне может поджидать сюрприз, который наверняка будет не единственным.

Случай индикации номера едва ли проще, поскольку необходимо отличать услугу индикации номера звонящего (CLIP) от услуги передачи или запрета на передачу собственного номера во время каждого звонка (CLIR).

Очевидно, что наличие как одной, так и другой услуги зависит от решения оператора и, следовательно, от выбираемой тарифной схемы. В принципе достаточно набрать *#30#, чтобы узнать, имеется ли услуга индикации номера звонящего.

Соответственно, можно разрешить передачу собственного номера, аннулируя от звонка к звонку услугу CLIR. Для этого перед номером набирается префикс *31#. И наоборот, иногда можно запрещать от звонка к звонку передачу по умолчанию своего номера. В этом случае при помощи префикса #31# временно запускается услуга CLIR.

Само собой разумеется (хотя об этом мало говорится), номера, записанные в телефонную книжку, вполне могут содержать подобные префиксы, и, таким образом, использовать анонимность «карты».

Скрытые команды

Практически все мобильные телефоны имеют «скрытые» команды, позволяющие техническим специалистам входить в предназначенные для них секретные меню. Операционный режим изменяется от одной марки телефона к другой, начиная с простой последовательности «меню – звездочка» некоторых моделей SAGEM до 000000* большинства моделей Alcatel.

Всю эту «секретную» информацию, регулярно обновляемую по мере появления новых моделей, можно найти в сети Internet.

Конечно, никто не имеет права запретить владельцу мобильного телефона набирать любую комбинацию цифр и команд на клавиатуре

(возможно, даже наугад), но все-таки настоятельно рекомендуется соблюдать предельную осторожность.

Некоторые меню настройки могут предлагать выполнение действий, которые способны привести к лишению гарантий производителя и даже нарушению работы сетей. Осознавая такую опасность, компания Motorola решила предоставить доступ к этим меню только через подключение специальной SIM-карты, называемой test-картой (см. рис. 3.17).

Ниже будет показано, как можно создать своего рода «ключ», позволяющий, помимо всего прочего, считывать некоторые конфиденциальные коды.

Существуют мобильные телефоны с различными функциями «отслеживания» сетей, способные выдавать идентификационные номера сот, обслуживающих определенную местность, и даже измерять интенсивность полученного сигнала, а также расстояние между базовыми станциями и мобильным телефоном (см. рис. 3.18).

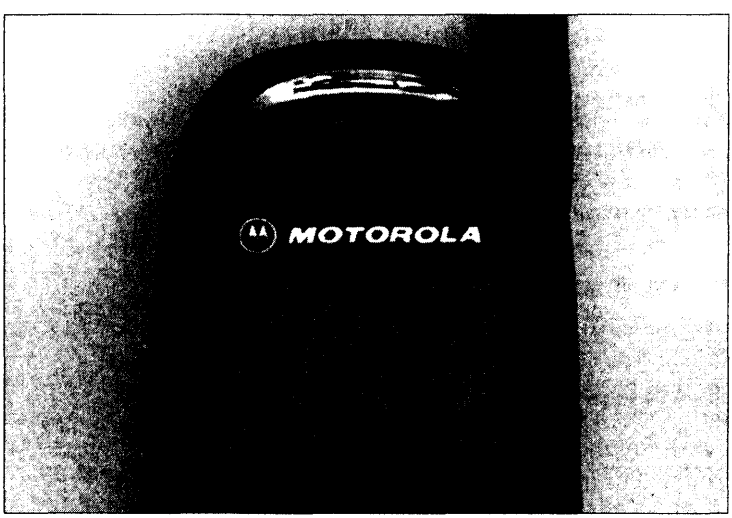


Рис. 3.17. Режим тестирования test позволяет считывать некоторые секретные коды

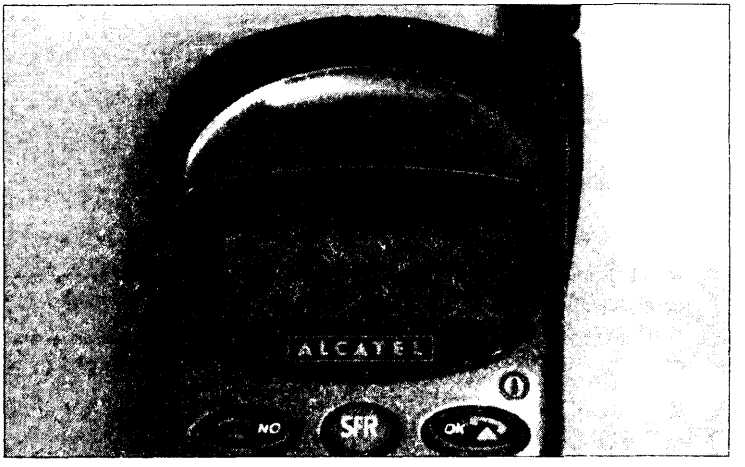


Рис. 3.18. Режим отслеживания trace позволяет идентифицировать базовые станции

4 НАБОР ИНСТРУМЕНТОВ GSM

Для более детального изучения возможностей мобильных телефонов GSM и сетей, которые их обслуживают, нельзя ограничиться только введением при помощи клавиатуры простых команд, пусть даже и специальных.

В данной главе рассматриваются технические и программные средства, необходимые для перехода к более глубокому исследованию. Они предназначены для самостоятельного использования в отличие от инструментария, предлагаемого торгово-промышленными фирмами, который подробно представлен в главе 5.

Здесь также описывается, как самостоятельно изготовить различные аксессуары, весьма полезные при повседневном использовании мобильного телефона. При этом соотношение функции/цена у данных аксессуаров значительно лучше по сравнению с аксессуарами, существующими на рынке.

4.1. ДЕТЕКТОР – ПОВТОРИТЕЛЬ ЗВОНКА

В схеме данного детектора используется тот же принцип, что и в автономных вибраторах, которые предназначены для мобильных телефонов, изначально не оснащенных ими.

Может показаться странным, что это устройство (см. рис. 4.1) включается значительно раньше, чем начинает звонить мобильный телефон.

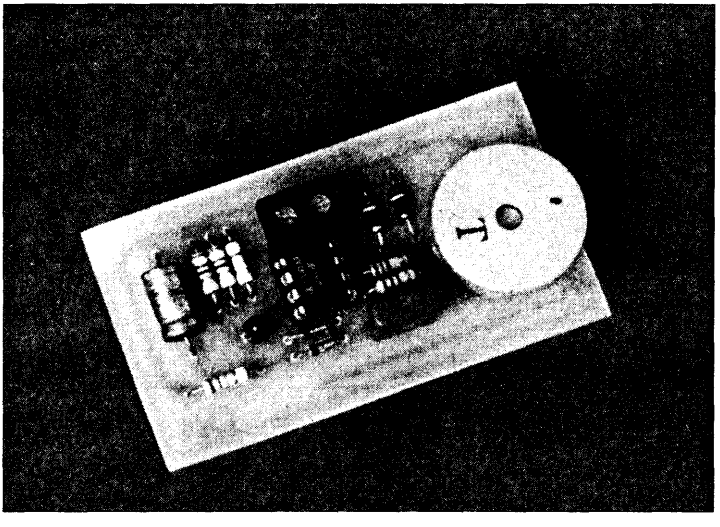


Рис. 4.1. Внешний вид собранной платы детектора звонка

Это объясняется тем, что детектор обнаруживает пакет битов, который передается телефоном в сеть в подтверждение его готовности ответить на поступивший звонок.

Такие устройства могут включаться и в других ситуациях, когда мобильный телефон отправляет в сеть достаточно длинный пакет битов (имеется в виду включение и выключение телефона, прием и передача данных, SMS-сообщений или голосовых сообщений).

И наоборот, обмен информацией, происходящий при смене соты или в ответ на запрос аутентификации, как правило, слишком короток, чтобы вызвать включение детектора.

В схеме детектора, представленной на рис. 4.2, используется действие мощных электромагнитных помех, которые создаются работающим мобильным телефоном в непосредственной близости от него.

В то время как производители и операторы мобильной связи не устают говорить о безвредности мобильных телефонов (или скорее недостатке формальных доказательств их вреда), применение схемы данного детектора даст читателям хорошую возможность самим объективно оценить степень воздействия мобильных телефонов.

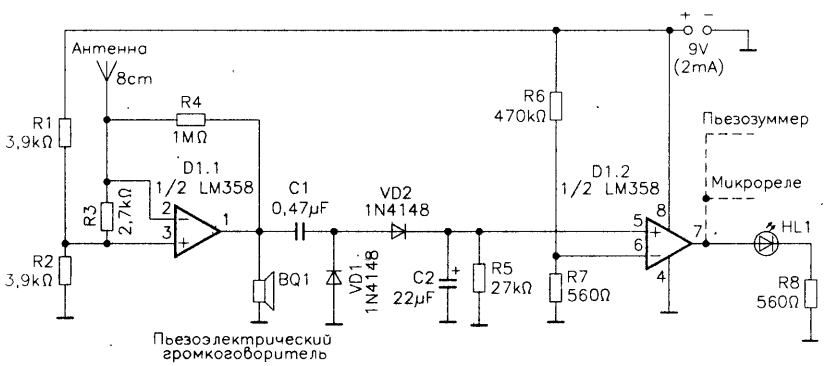


Рис. 4.2. Схема детектора звонка

На расстоянии нескольких десятков сантиметров напряженность поля, создаваемого мобильным телефоном, достаточна для наведения в антенне, размеры которой соответствует используемой частоте, ЭДС величиной десятки или сотни милливольт. Примером такой антенны может служить простой неэкранированный провод длиной 2, 4 или 8 см (не более). При подключении этого провода к элементу, выполняющему функции детектирования, выделяется огибающая

СВЧ сигнала, обычно имеющая вид импульсов звуковой частоты, прекрасно поддающихся усилению.

В современных качественных телефонах строгое соблюдение требований, касающихся ЭМС (электромагнитной совместимости), например, в предварительном усилителе звука, позволяет добиться приемлемой устойчивости относительно рассматриваемых помех.

К сожалению, этого нельзя сказать о более старых аппаратах, даже если они прекрасно работают, и, само собой разумеется, об огромном количестве дешевых устройств.

Внутри интегральных схем имеется множество полупроводниковых переходов, которые, как правило, и играют роль детекторов мощных СВЧ импульсов, излучаемых мобильным телефоном.

Первый каскад операционного усилителя, представленного на схеме, является примером того, что, как правило, никогда не следует делать: каскад имеет большое усиление, и при этом его вход практически является открытым (то есть входное сопротивление достаточно велико). Чтобы еще больше «усугубить» ситуацию (увеличить чувствительность схемы), предусмотрено в качестве входной антенны использовать проводник такой длины (8 см), чтобы схема была приблизительно настроена на соответствующие частоты работы мобильного телефона.

Небольшой пьезоэлектрический громкоговоритель, который может подключаться к выходу усилителя, должен издавать характерное гудение, как только в радиусе менее 50 см – 1 м от него начинает работать мобильный телефон GSM.

Наибольшее беспокойство вызывает тот факт, что такой пьезоэлектрический элемент, даже не подключенный к чему-либо, часто начинает издавать звук, если он находится только в нескольких сантиметрах от антенны. Это означает, что при обычном использовании аппарата его излучение воздействует на органы слуха и жизненно важные зоны мозга.

Некоторым людям, обладающим достаточно чувствительным слухом, удается уловить сигналы, исходящие от мобильного телефона, даже если его динамик не издает совершенно никаких звуков. Говорят, что это явление связано с непосредственной реакцией органов слуха на электромагнитные поля сильной интенсивности. В некоторых исследованиях делается следующий вывод: чтобы работа телефона не представляла никакого риска для здоровья, он должен находиться на расстоянии не менее... 12 метров от уха!

Второй каскад схемы преобразует полученный сигнал в импульсную информацию, которую проще использовать на практике. Выпрямитель/удвоитель напряжения соединен со вторым операционным

усилителем, включенным по схеме компаратора, сигнал на выходе которого может управлять различными устройствами.

На первых порах, чтобы немного поэкспериментировать, будет достаточно использовать обычный светодиод, но впоследствии можно его заменить на пьезоэлектрический зуммер (со встроенным генератором) или даже на небольшое реле. Последний вариант хорошо подходит для выполнения схемы «повторителя звонка», способной управлять, например, соответствующим сигнальным устройством в автомобиле или каким-либо устройством дистанционного управления.

На рис. 4.3 представлена топология печатной платы, где намеренно игнорируются самые элементарные правила электромагнитной совместимости. Соответственно, воздействие ВЧ излучения, которое надо обнаружить, будет только усилено.

При необходимости можно несколько изменить печатную плату, чтобы адаптировать ее для конкретного случая использования, или, напротив, строго придерживаться схемы размещения элементов, представленной на рис. 4.4. Перечень элементов к схеме приведен в табл. 4.1.

В качестве одного из вариантов можно рассмотреть схему управления с использованием небольшого реле. Топология печатной платы

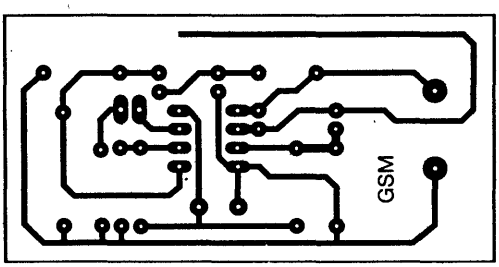


Рис. 4.3. Топология печатной платы детектора звонка

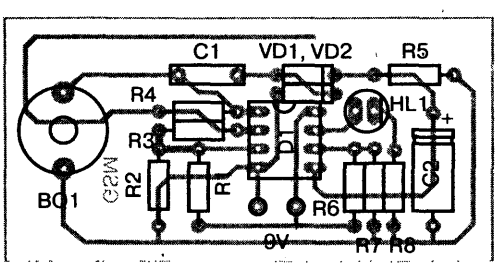


Рис. 4.4. Схема размещения элементов детектора звонка

Таблица 4.1. Перечень элементов к рис. 4.4

Наименование	Обозначение	Номинал	Примечание
Резисторы	R1, R2	3,9 кОм	
	R3	2,7 кОм	
	R4	1 МОм	
	R5	27 кОм	
	R6	470 кОм	
	R7, R8	560 Ом	
Конденсаторы	C1	0,47 мкФ	
	C2	22 мкФ × 16 В	Электролитический, горизонтальное исполнение
Интегральные микросхемы	D1	LM358	
Диоды	VD1, VD2	1N4148	
	HL1		Красный светодиод
Прочие	BQ1 – пьезоэлектрический громкоговоритель типа KBS 20 DB 4P Murata		
	Элемент питания 9 В		

показана на рис. 4.5, а размещение элементов монтажа – на рис. 4.6. Перечень элементов приведен в табл. 4.2, а внешний вид собранной платы – на рис. 4.7.

Питание схемы в обоих вариантах осуществляется от миниатюрной батарейки на 9 В, размеры которой хорошо сочетаются с размерами печатной платы. При этом обеспечивается требуемая автономность работы (потребление в режиме ожидания 2 мА). Конечно, при необходимости можно использовать и другой источник питания (например, аккумулятор автомобиля).

В случае же стационарной работы оборудования можно воспользоваться существующей в помещении стандартной электрической сетью, но, безусловно, тщательно стабилизировав и отфильтровав напряжение, поскольку следует учитывать высокую чувствительность данного устройства.

Работоспособность собранной схемы можно проверить, позвонив с мобильного телефона GSM, находящегося в непосредственной близости. В принципе, срабатывание детектора звонка возможно на расстоянии до 50 см, а в случае максимальной излучаемой мощности – до 1 м. В действительности следует знать, что мобильные телефоны постоянно автоматически адаптируют свою излучаемую мощность к уровню, который является достаточным для обеспечения устойчивой связи с базовой станцией.

Таблица 4.2. Перечень элементов к рис. 4.5

Наименование	Обозначение	Номинал	Примечание
Резисторы	R1, R2	3,9 кОм	
	R3	2,7 кОм	
	R4	1 МОм	
	R5	27 кОм	
	R6	560 Ом	
	R7	560 кОм	
	R8	680 Ом	
	R9	180 Ом	
Конденсаторы	C1	0,47 мкФ	
	C2	22 мкФ × 16 В	Вертикальное исполнение
	C3	100 мкФ × 16 В	Вертикальное исполнение
Интегральные микросхемы	D1	LM358	
	D2	2N 2222	
Диоды	VD1, VD2, VD3	1N4148	
	HL1		Красный светодиод
Прочие	Реле DIL на 12 В		
	Две колодки клеммные на два контакта (5,08 мм)		

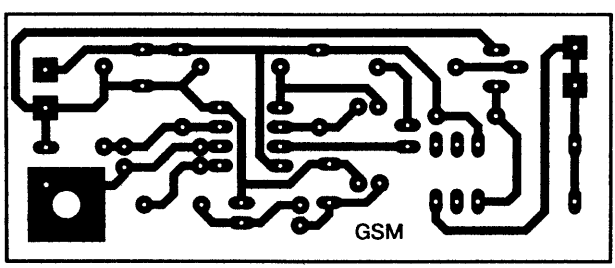


Рис. 4.5. Топология печатной платы детектора звонка при использовании реле

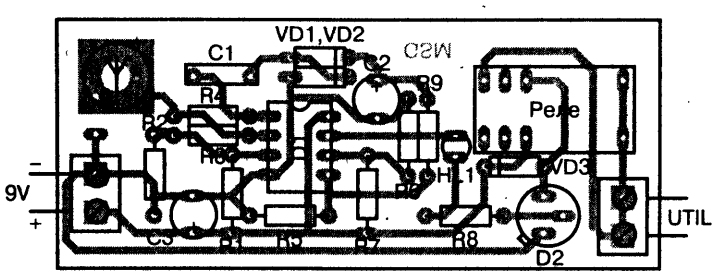


Рис. 4.6. Схема размещения элементов при топологии по рис. 4.5

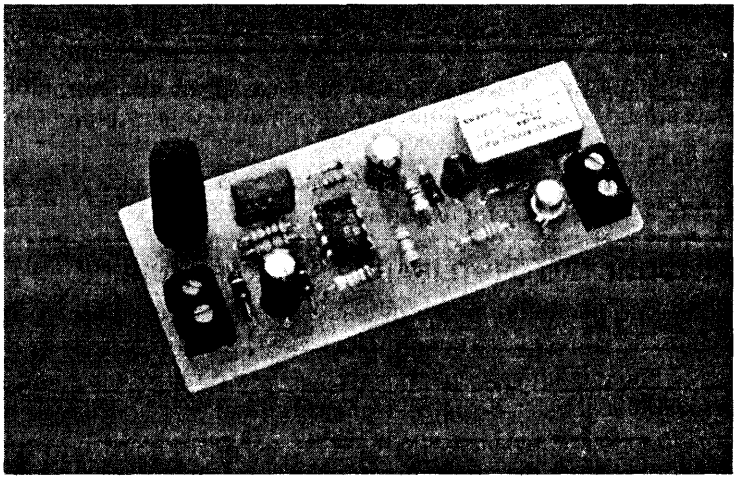


Рис. 4.7. Внешний вид собранной платы детектора звонка с использованием реле

В зоне уверенного покрытия мощность может быть значительно снижена, что позволяет, помимо прочего, увеличить автономность работы аккумуляторной батареи. В этом случае может показаться, что данная схема (или любой другой автономный вибратор) стала менее чувствительной. Чтобы гарантировать надежность оптимального срабатывания, лучше расположить собранное устройство как можно ближе к мобильному телефону, например, на расстоянии от 10 до 20 см.

Следует заметить, что схема способна детектировать и другие ВЧ импульсы, излучаемые не только мобильными телефонами. Она должна срабатывать, в частности, при приближении к дверце работающей микроволновой печи, даже если последняя и экранирована. Наблюдение такого рода позволяет в некотором смысле подтвердить опасения, возникающие в отношении влияния работающих мобильных телефонов на здоровье.

Согласно исследованиям, двадцать минут непрерывной работы телефона вызывает локальное повышение температуры головного мозга на один градус! Следовательно, становится сопоставимым влияние облучений от телефона и от микроволновой печи, держаться от которой во время ее работы рекомендуется подальше.

Зато можно не беспокоиться из-за возможного вредного воздействия антенн базовых станций. Вне их главного сектора излучения (который располагается непосредственно перед антенной и мощность излучения в котором составляет несколько сотен ватт) электромагнитное

излучение практически отсутствует. Поэтому, для того чтобы собранная схема среагировала, необходимо расположить ее очень близко к излучающей антенне. Следовательно, находиться под антенной базовой станции или за ней намного безопасней, чем регулярно и долго говорить по мобильному телефону.

Может быть, это небольшое и несложное по монтажу устройство вдохновит вас на дальнейшие исследования.

4.2. УСТРОЙСТВО СЧИТЫВАНИЯ SIM-КАРТ ДЛЯ ПК

Самые интересные манипуляции с мобильным телефоном требуют считывания и записи информации на его SIM-карте.

Эта тема подробно разбирается в главе 5, где также представлены различные необходимые для ее реализации пакеты программ, которые можно найти в продаже.

Здесь же ограничимся описанием того, как изготовить предельно упрощенное считывающее устройство, которое в сочетании с любым IBM-совместимым ПК, способным работать в MS DOS 3.30 или выше, позволит провести множество очень интересных экспериментов (естественно, под полную ответственность пользователя).

Любое устройство для считывания чип-карт протокола T = 0 теоретически позволяет выполнить любые манипуляции, однако гораздо проще и удобнее воспользоваться специальным инструментарием.

Будучи асинхронной чип-картой, SIM-карта мобильного телефона является настоящим микрокомпьютером, обладающим центральным процессором, памятью, периферийными устройствами и программным обеспечением. Она общается со считывающим устройством (или терминалом), в котором размещается, при помощи двунаправленной последовательной шины данных, в то время как ее работа синхронизируется внешним тактовым генератором.

Для «общения» с асинхронными картами было разработано множество протоколов, однако самым распространенным является протокол T = 0. Наличие в нем многих точек соприкосновения с протоколом RS-232 позволяет добиться совершенно удивительных результатов «в обход» обычного последовательного порта благодаря простейшей схеме сопряжения (интерфейса).

Как правило, устройства для считывания асинхронных карт построены на микроконтроллере, в котором запрограммирована настоящая операционная система (иногда говорят об операционной системе считывающего устройства ROS – Reader Operating System).

Поскольку такое соединительное устройство является очень сложным и дорогостоящим, часть его наиболее важных функций можно перенести на уровень программ, выполняемых ПК, что позволит свести вопросы технического обеспечения к минимуму.

Таким образом, в состав схемы, представленной на рис. 4.8, входит стабилизатор напряжения (5 В), тактовый генератор (3,58 МГц), а также несколько буферов, задача которых – согласование уровней напряжения и разделение входящих (TXD) и выходящих данных (RXD).

Топология односторонней печатной платы приведена на рис. 4.9, схема размещения элементов – на рис. 4.10, а перечень элементов –

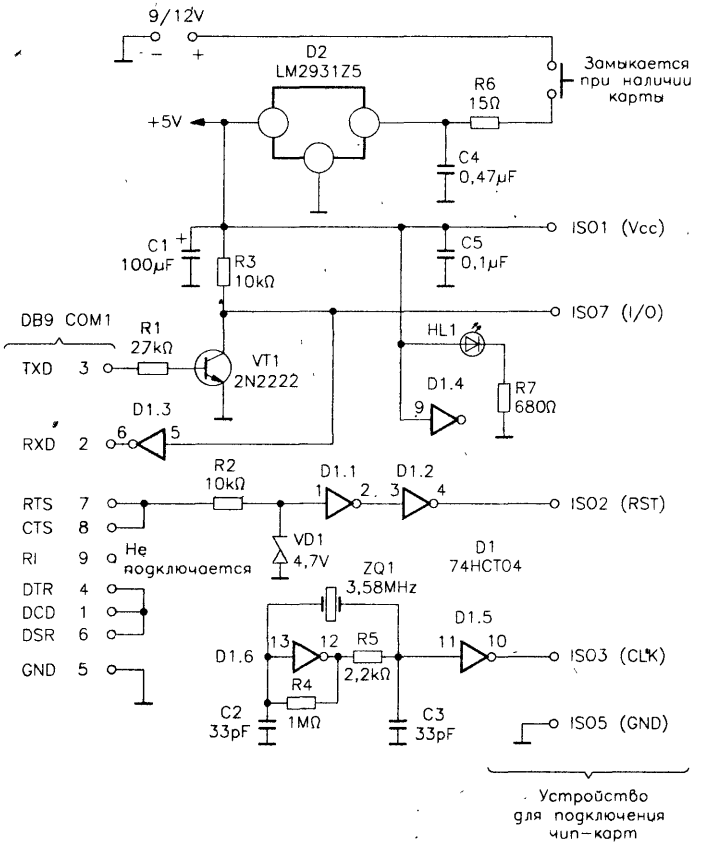


Рис. 4.8. Принципиальная схема устройства считывания SIM-карт

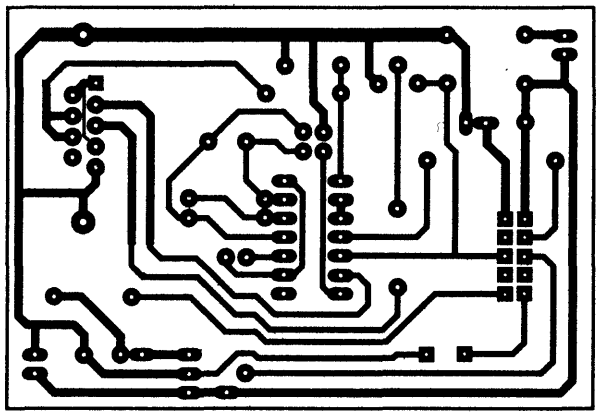


Рис. 4.9. Топология печатной платы устройства считывания SIM-карт

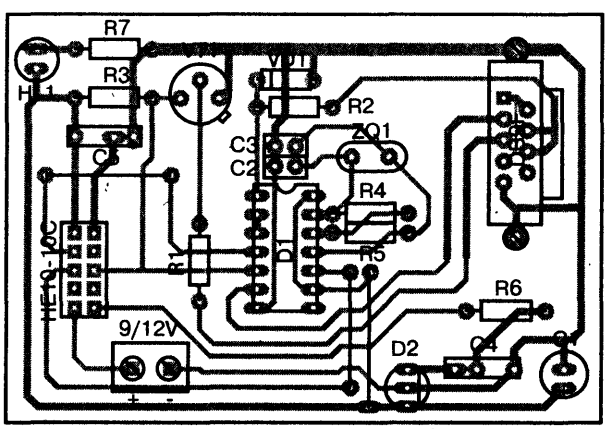


Рис. 4.10. Схема размещения элементов устройства считывания SIM-карт

в табл. 4.3. Собранная печатная плата (см. рис. 4.11) подключается к источнику питания (элемента питания 9 В может быть вполне достаточно), а также к последовательному порту ПК (COM1 или COM2 в зависимости от приложений).

Для этого используется кабель, так называемый удлинитель для монитора, соединяющий контакт в контакт разъем DB9 типа «вилка» с разъемом DB9 типа «розетка», хотя можно подключить схему к последовательному порту ПК и напрямую.

Таблица 4.3. Перечень элементов к рис. 4.10

Наименование	Обозначение	Номинал	Примечание
Резисторы	R1	27 кОм	
	R2	10 кОм	
	R3	10 кОм	
	R4	1 МОм	
	R5	2,2 кОм	
	R6	15 Ом	
	R7	680 Ом	
Конденсаторы	C1	100 мкФ × 10 В	Электролитический, вертикальное исполнение
	C2	33 пФ	
	C3	33 пФ	
	C4	0,47 мкФ	
	C5	0,1 мкФ	
Интегральные микросхемы	D1	74 HCT 04	
	D2	LM 2931 Z 5	
Полупроводники	HL1		Красный светодиод
	VD1	4,7 В/0,25 Вт	Стабилитрон
	VT1	2N 2222	
Прочее	ZQ1	3,58 (или 3,579) МГц	Кварцевый резонатор
	Колодка клеммная на два контакта (5,08 мм)		
	Разъем DB9 – розетка		
	Картоприемник (ITT – CANNON)		
	Разъемная колодка с двумя рядами квадратных угловых штырьков		
	Два десятиконтактных разъема HE10 с заправкой плоского 10-проводного кабеля длиной 10–20 см		
	Источник питания 9–12 В или элемент питания 9 В		
	Кабель «удлинитель для монитора» с разъемом DB9 вилка/розетка		

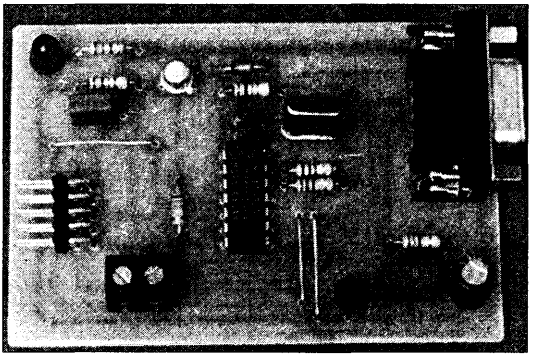


Рис. 4.11. Внешний вид собранной основной печатной платы устройства считывания SIM-карт

Картоприемник (модель марки ITT-CANNON с контактом NO[1], замыкающимся при вставлении карты) подключается к дополнительной плате, топология которой приведена на рис. 4.12, а схема размещения элементов – на рис. 4.13 (следует обратить внимание на пять перемычек, которые надо будет припаять в первую очередь).

Соединение этих двух модулей производится при помощи широко распространенного разъема HE10. При этом используются двухрядные разъемные колодки с квадратными угловыми штырьками и плоский кабель с двумя десятиконтактными розетками HE10, их ключи должны быть направлены в одну сторону, а соединение производиться контакт в контакт. Подобного рода соединение гарантирует совместимость с инструментальным комплектом, описанным в моей книге «Чип-карты: Устройство и применение в практических конструкциях» (М.: ДМК, 2000).

Внешний вид собранной дополнительной платы с картоприемником приведен на рис. 4.14.

Так как в данном картоприемнике используются только те контакты, которые необходимы для работы асинхронных карт, его не рекомендуется применять в любой другой схеме, предназначенной для синхронных карт (например, для телевизионных карт).

Программы INVISO.EXE и DIRISO.EXE, необходимые для использования устройства считывания, содержатся на компакт-диске в каталоге LECTSIM. Обе они требуют того, чтобы описанная выше схема была подключена к последовательному порту COM1 ПК, по возможности освобожденному (с точки зрения программного и технического обеспечения). Запуск указанных программ производится в MS DOS, поэтому для их работы достаточно ранних моделей ПК (например, 386 SX 25) и нет необходимости в наличии Windows.

Приведенные ниже исходные тексты программ также содержатся в каталоге BASIC. Не следует пытаться запускать их в простом интерпретаторе GWBASIC или QBASIC. Если в исходный текст вносятся какие-либо изменения (например, вместо COM1 используется COM2), то необходимо откомпилировать его с помощью Turbo Basic (этот вопрос подробно рассматривается в моей книге «BASIC pour microcontrôleurs et PC»).

```
10 REM ---- INVISO.BAS ----
20 KEY OFF:CLS
```

[1] Сокращение NO (Normally Open – нормально разомкнутый) используется для обозначения замыкающегося контакта и т.п. – *Прим. науч. ред.*

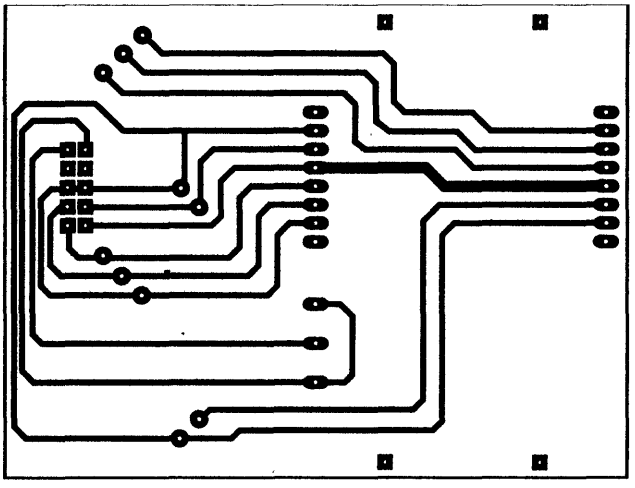


Рис. 4.12. Топология дополнительной печатной платы для подсоединения картоприемника

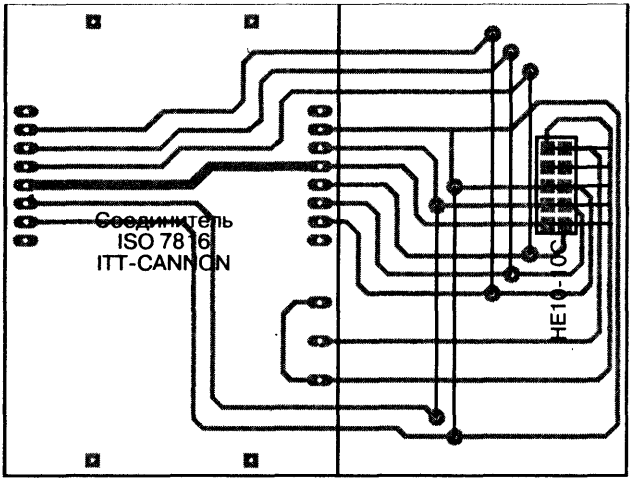


Рис. 4.13. Схема размещения элементов на дополнительной плате для подсоединения картоприемника марки ITT-CANNON с замыкающимся контактом

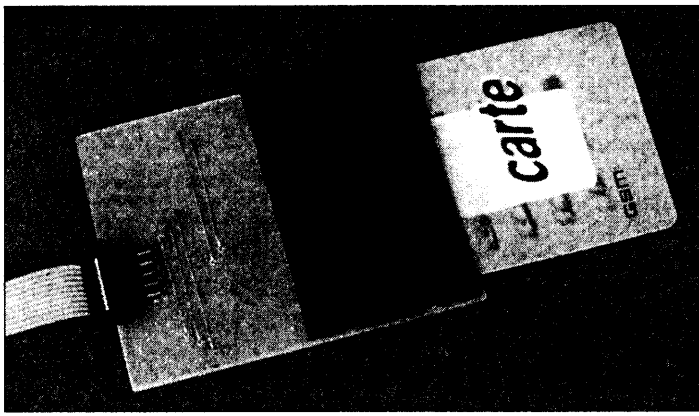


Рис. 4.14. Внешний вид собранной дополнительной платы с картоприемником

```
30 PRINT"Диалог с картами по обратному соглашению ISO"
40 PRINT:PRINT
50 OPEN "COM1:9600,o,8,2" AS #1
60 PRINT"Вставить карту и ввести команду ISO"
70 PRINT"ESCAPE для выхода":PRINT
80 GOSUB 110
90 PRINT #1,M$;:NL$=INPUT$(LEN(M$),#1)
100 GOTO 80
110 M$=""
120 A$=INKEY$:IF A$<>"" THEN 150
130 IF LOC(1)<>0 THEN GOSUB 230
140 GOTO 120
150 IF A$=CHR$(27) THEN END
160 PRINT A$;
170 B$=INKEY$:IF B$="" THEN 170
180 PRINT B$+" ";
190 N=VAL("&H"+A$+B$)
200 GOSUB 370
210 M$=CHR$(M)
220 RETURN
230 T$=TIME$
240 IF T$=TIME$ THEN 240
250 IF LOC(1)=0 THEN RETURN
260 C$=INPUT$(LOC(1),#1): PRINT : PRINT " * ";
270 FOR K=1 TO LEN(C$)
```

```
280 N=ASC(MID$(C$,K,1))
290 GOSUB 370
300 D$=HEX$(M)+" "
310 IF LEN(D$)<3 THEN D$="0"+D$
320 PRINT D$;
330 NEXT K
340 IF LOC(1)<>0 THEN C$=INPUT$(LOC(1),#1):GOTO 270
350 PRINT "*"
360 RETURN
370 M=255
380 IF N>127 THEN N=N-128:M=M-1
390 IF N>63 THEN N=N-64:M=M-2
400 IF N>31 THEN N=N-32:M=M-4
410 IF N>15 THEN N=N-16:M=M-8
420 IF N>7 THEN N=N-8:M=M-16
430 IF N>3 THEN N=N-4:M=M-32
440 IF N>1 THEN N=N-2:M=M-64
450 IF N>0 THEN M=M-128
460 RETURN
470 REM (c)1997, 1999 Patrick GUEULLE
```

```
10 REM ---- DIRISO.BAS ----
20 KEY OFF:CLS
30 PRINT"Диалог с картами по прямому соглашению ISO"
40 PRINT:PRINT
50 OPEN "COM1:9600,e,8,2" AS #1
60 PRINT"Вставить карту и ввести команду ISO"
70 PRINT"ESCAPE для выхода":PRINT
80 GOSUB 110
90 PRINT #1,M$;:NL$=INPUT$(LEN(M$),#1)
100 GOTO 80
110 M$=""
120 A$=INKEY$:IF A$<>"" THEN 150
130 IF LOC(1)<>0 THEN GOSUB 210
140 GOTO 120
150 IF A$=CHR$(27) THEN END
160 PRINT A$;
170 B$=INKEY$:IF B$="" THEN 170
180 PRINT B$+" ";
190 M$=CHR$(VAL("&H"+A$+B$))
200 RETURN
210 T$=TIME$
220 IF T$=TIME$ THEN 220
230 IF LOC(1)=0 THEN RETURN
```

```
240 C$=INPUT$(LOC(1),#1): PRINT : PRINT " * ";
250 FOR K=1 TO LEN(C$)
260 D$=HEX$(ASC(MID$(C$,K,1)))+" "
270 IF LEN(D$)<3 THEN D$="0"+D$
280 PRINT D$;
290 NEXT K
300 IF LOC(1)<>0 THEN C$=INPUT$(LOC(1),#1):GOTO 250
310 PRINT "*"
320 RETURN
330 REM (c)1997, 1999 Patrick GUEULLE
```

Программа INVISO.EXE позволяет проводить любые манипуляции с картами, работающими по обратному соглашению (ответ на сброс начинается с байта 3Fh). Для карт, работающих по прямому соглашению (ответ на сброс начинается с байта 3Bh), используется программа DIRISO.EXE.

Как только карта вставлена в устройство для считывания (по приглашению, поступившему от программы), она непроизвольно выдает группу байтов – ответ на сброс, или ATR (Answer To Reset). Этот ответ появляется на экране, и часто он оканчивается на 90 00 (но это не обязательно).

Затем карта ждет команд, которые необходимо ввести с клавиатуры. Все ответы карты будут постепенно отображаться на экране в окружении звездочек (во избежание путаницы с тем, что набиралось на клавиатуре).

Любая команда протокола T = 0 состоит из заглавного блока (заголовка) из пяти байт, за которым следует блок данных. Все выражается в шестнадцатеричном формате. Пять байт заголовка соответственно именуются CLA, INS, P1, P2 и LEN и представляют собой следующее:

- CLA – «класс» карты, например, BCh для банковской карты или карты VITALE, и A0h для SIM-карты;
- INS – операционный код команды, которую должна выполнить карта. Для SIM-карт эти коды уже были рассмотрены в главе 3 (см. раздел «SIM-карта»);
- P1 и P2 уточняют, что должна делать карта, или по умолчанию остаются в виде 00 00;
- LEN указывает длину блока данных, посылаемых карте или ожидаемых от нее.

В случае «входящей» команды байты данных отправляются после кода LEN, но только после того, как карта ответила байтом процедуры (часто это бывает просто повторением операционного кода команды).

В случае «выходящей» команды блок данных посылается картой по получении байта LEN и передачи байта процедуры. Практически во всех случаях карта завершает выполнение команды отправкой двух байт отчета (SW1 и SW2). Если все прошло удачно, то отчет будет послан в виде 90 00.

Таким образом, с SIM-картой можно сделать многое. Но следует иметь в виду, что некоторые некорректные манипуляции могут надолго или окончательно заблокировать карту или даже повредить ее физически.

Стандарт GSM 11.11 содержит детальное описание файлов и команд, позволяющих проводить операции считывания и записи. Этот вопрос будет рассмотрен в следующей главе.

Прежде всего необходимо ввести (или просто нейтрализовать раз и навсегда) конфиденциальный код, защищающий доступ к карте (тот, который обычно набирается во время каждого включения телефона).

Предположим, что кодом является 1234 (в новой карте 0000). Переведем код ASCII в шестнадцатеричный формат и дополним его до восьми цифр, набрав FFh. Получим:

```
31 32 33 34 FF FF FF FF
```

Чтобы представить код карте (после получения ее ответа на сброс), набираем:

```
A0 20 00 01 08
```

Как только карта ответит 20 (байт процедуры), введем:

```
31 32 33 34 FF FF FF FF
```

Если код верный, то в ответ карта отправит 90 00. Если код уже был дезактивирован и карте больше не нужен – 98 08.

Чтобы дезактивировать этот код, только создающий неудобства для проводимых экспериментов, можно набрать следующее:

```
A0 26 00 01 08
```

Затем, после получения байта 26, введите:

```
31 32 33 34 FF FF FF FF
```

Код всегда можно снова активировать, если набрать:

```
A0 28 00 01 08
```

А затем, после получения байта 28, опять ввести:

```
31 32 33 34 FF FF FF FF
```

Помимо этих манипуляций, которые без труда можно выполнить при помощи разработанных мною программ, приведенных в данной книге, рассматриваемое устройство для считывания вполне совместимо с некоторыми общедоступными программами, такими как SimScan, которую можно найти в Internet. Эта программа в нескольких вариантах содержится на компакт-диске в каталоге INTERNET.

4.3. «ШПИОН» ЗА SIM-КАРТАМИ

Эксперименты с SIM-картами могут послужить прекрасным источником вдохновения. Очень интересно наблюдать «диалог», который завязывается между мобильными телефонами и SIM-картой. Достаточно взять небольшое количество электронных компонентов и использовать очень простое программное обеспечение, чтобы полностью удовлетворить законное любопытство.

В большинстве случаев этот двухсторонний поток данных циркулирует со скоростью 9600 бод и проходит через контакт ISO7 SIM-карты. Перехваченный электронной схемой, включенной в параллель, он может быть легко декодирован через UART последовательного порта ПК, если хитро «подогнать» параметры.

Для такой схемы можно использовать широко распространенную микросхему MAX 232, как показано на рис. 4.15. Она осуществляет согласование уровней напряжения между чип-картой и линией

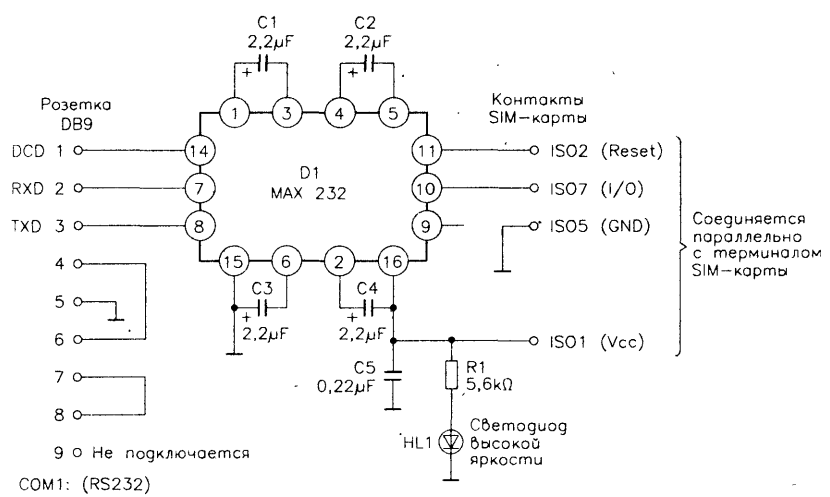


Рис. 4.15. Принципиальная схема «шпиона» за SIM-картами

последовательного интерфейса RS232. Не очень требовательная к электроэнергии, приведенная схема напрямую питается от мобильного телефона, при этом еще остается энергия для светодиода «высокой яркости», позволяющего визуализировать фазы активирования и дезактивирования карты. Кроме посылаемых и принимаемых картой и телефоном данных, микросхема MAX 232 снимает также сигнал сброса (reset) карты, используемый программным обеспечением для точной самосинхронизации.

Топология печатной платы выполняется согласно рис. 4.16. Размещение элементов монтажа показано на рис. 4.17, а перечень элементов приведен в табл. 4.4.

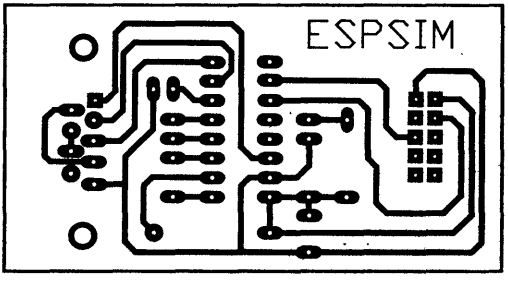


Рис. 4.16. Топология печатной платы интерфейсного модуля

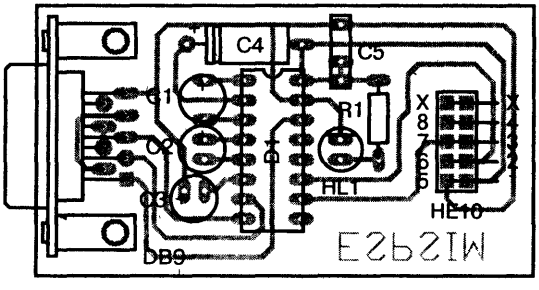


Рис. 4.17. Схема размещения элементов на плате интерфейсного модуля

Собранная плата этого интерфейсного модуля (см. рис. 4.18) соединяется затем с мобильным телефоном и его SIM-картой. Делается это при помощи четырех проводов, подключаемых к контактам ISO1 (V_{cc}), ISO2 (Reset), ISO5 (земля) и ISO7 (данные). Контакт сигнала тактовой частоты ISO3 при этом не используется.

Таблица 4.4. Перечень элементов к рис. 4.17

Наименование	Обозначение	Номинал	Примечание
Резисторы	R1	5,6 кОм	(зеленый, синий, красный)
Конденсаторы	C1, C2, C3	2,2 мкФ × 16 В	Вертикальное исполнение
	C4	2,2 мкФ × 16 В	Горизонтальное исполнение
	C5	0,22 мкФ × 63 В	
Интегральные микросхемы	D1	MAX 232	
Диоды	HL1		Красный светодиод высокой яркости
Прочее	Разъем DB9 – розетка		
	Разъем HE10 на 10 контактов или разъемная колодка		

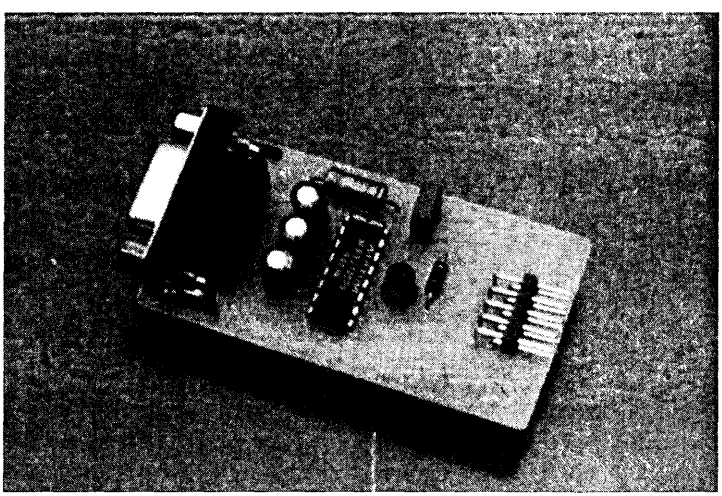


Рис. 4.18. Внешний вид собранной платы интерфейсного модуля

Если у вас сохранился старый мобильный телефон, вы можете использовать его для проведения различных экспериментов. Например, имеет смысл просто подпаять указанные провода параллельно контактам разъема SIM-карты. Однако более элегантным было бы подсоединение через контактные адаптеры, которые позволяют расширить ваши исследовательские возможности (осуществлять манипуляции при подключении к различным моделям телефонов или автономным считывающим устройствам для SIM-карт). Для этого можно оснастить плату контактным разъемом типа HE10 на 10 контактов (обычный

кусок контактной колодки с двумя рядами квадратных угловых штырьков).

Затем надо изготовить специальный соединительный кабель. Для этого подойдет отрезок плоского 10-жильного кабеля длиной приблизительно 20 см, на котором закрепляются три ответных разъема HE10, соединенных параллельно контакт в контакт (см. рис. 4.19).

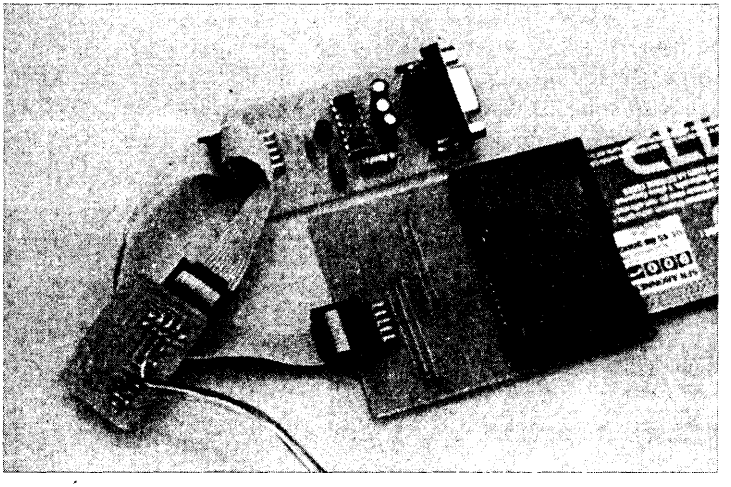


Рис. 4.19. Различные элементы схемы «шпиона» за SIM-картами

Таким образом, автоматически обеспечивается совместимость не только с соединителем, изображенным на рис. 4.13, но и «фальш-картами» из текстолита 8/10 мм, описанными в моей книге «Cartes a puce initiation et applications» («Чип-карты. Устройство и применение в практических конструкциях»).

Следует отметить, что SIM-карты формата «микро» могут вставляться в промышленно выпускаемые адаптеры, которые придают им полный формат «ISO». Можно также временно снова склеить куски карты при помощи клейкой ленты (или прикрепить к оставшейся настоящей карте).

Остается подсоединить телефон при помощи «фальш-карты», изготовленной из текстолита 8/10 мм, на одной стороне которой вытравлены соответствующие контактные дорожки. Разумеется, точная форма такого адаптера зависит от модели телефона.

«Фальш-карта», приведенная на рис. 4.20, подходит для некоторых моделей марки SAGEM, начиная с RC712.

Вставка «фальш-карты» в телефон требует съема и повторной установки нижней части корпуса, закрепленной только четырьмя винтами типа TORX N°6 под миниотвертку. Провода должны быть достаточно тонкими и гибкими, чтобы их можно было пропустить между батареей и крышкой корпуса телефона (см. рис. 4.21). Теперь SIM-карта стала для телефона внешним устройством. Для подсоединения проводов (длиной от 10 до 20 см, не более) можно изготовить небольшой адаптер, представляющий собой печатную плату (см. рис. 4.22), которая имеет такую же ответную часть контактного разъема HE10, как и другие части схемы.

Тщательно проверьте выполненные вами соединения. Если все сделано правильно, телефон должен работать как с обычной SIM-картой, так и с SIM-картой для тестирования (то есть с любой SIM-картой, если она не заблокирована). Теперь можно подсоединить интерфейсный модуль к последовательному порту COM1 любого совместимого компьютера.

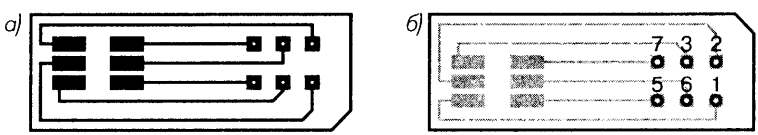


Рис. 4.20. Пример топологии «фальш-карты»

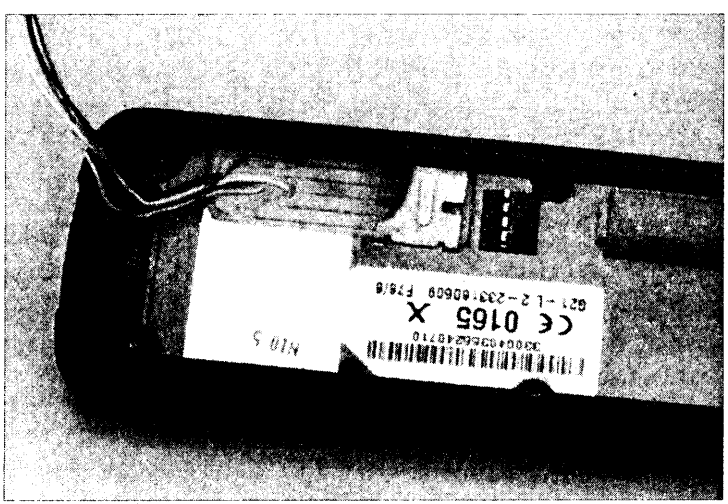


Рис. 4.21. Адаптер (фальш-карта), установленный в мобильный телефон

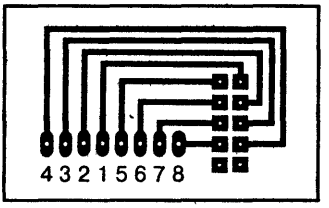


Рис. 4.22. Топология печатной платы адаптера

Обе программы, содержащиеся в каталоге ESPION на компакт-диске, являются приложениями DOS (SIMINV.EXE и SIMDIR.EXE). Это означает, что они могут работать даже на очень старых ПК (начиная с 386 SX 25). Если у вас более современный компьютер, необходимо полностью выйти из Windows, перед тем как запустить одну из программ. Можно также сразу включать компьютер со вставленной дискетой DOS. Действительно, некоторые версии Windows (например, NT или Millennium) препятствуют прямому доступу к портам ввода/вывода, которые как раз и необходимы. Исходный код программ находится в том же каталоге, так что при желании можно внести в него какие-либо изменения. Перед каждым использованием необходима также перекомпиляция файлов .EXE (см. мою книгу «BASIC pour microcontroleurs et PC»).

Одна из программ (SIMINV) предназначена только для SIM-карт, работающих по обратному соглашению (ответ на сброс начинается с 3Fh). Вторая (SIMDIR) – для карт, работающих по прямому соглашению (ответ на сброс начинается с 3Bh). Хотя использование несоответствующей программы и не приведет к каким-либо серьезным неполадкам, показания дисплея будут хаотичными до тех пор, пока программа не остановится по коду ошибки.

Отметим, что нажатие на клавишу ESCape позволяет выйти из программы.

После запуска и та, и другая программа ждет следующих важных указаний:

1. Какие действия выполнять после получения данных: по умолчанию (или при набранной команде «CON») выводить их на дисплей по мере перехвата, на печать (при наборе «PRN») или, что, на мой взгляд, предпочтительнее, записать их в файл «LOG» (набрав только его имя, без какого-либо расширения).
2. Надо ли вводить поправку, учитывая отклонение частоты тактового генератора от обычного значения 3,58 МГц, которое соответствует стандартной скорости передачи 9600 бит в секунду (следует по возможности проверить частоту при помощи цифрового частотомера, подключенного между контактом ISO3 и землей).

Например, для мобильного телефона RC712, в котором установлена карта с тактовой частотой 3,25 МГц, необходимо применить коэффициент подстройки 13 вместо коэффициента 12, используемого по умолчанию. Правда, остается неясным вопрос, для чего применяется такой нештатный режим работы: из целей «конспирации» или же это просто следствие некоторого разгона встроенного процессора.

Если все работает нормально, полученные данные выводятся в виде текста, состоящего из значений, которые представлены в шестнадцатеричном формате и разделены пробелами. Любая явная пауза в потоке данных вызывает переход на новую строку, что довольно часто (но не всегда) указывает на смену направления обмена данными (от мобильного телефона к SIM-карте или от SIM-карты к мобильному телефону).

Когда обмен данными осуществляется в высокоскоростном режиме, а используемый ПК не обеспечивает быстрый вывод данных, происходит переполнение (overflow) буфера последовательного порта (код ошибки 69). В таком случае лучше перейти к записи данных в файл .LOG, что будет рассматриваться позже. Отметим, что этот файл предпочтительнее размещать на виртуальном диске (RAMdrive), время доступа к которому очень мало. Интерпретация записанных таким образом сообщений предполагает хорошее знание прокола T = 0 и спецификации GSM 11.11, основные положения которой объясняются в главе 5.

Обратите внимание на следующий момент. Если сначала запустить программу, а затем подать питание на мобильный телефон (действуйте всегда только в таком порядке), то на дисплее должен высветиться (один или несколько раз) ответ SIM-карты на сброс. Если он не начинается с `3Fh` или `3Bh`, вполне вероятно, что программное обеспечение не соответствует типу карты (работа по прямому или обратному соглашению) или неправильно установлен коэффициент подстройки тактового генератора. Некоторые из SIM-карт последних выпусков могут на этом этапе стараться «договориться» с терминалом об изменении частоты тактового генератора – маневр, успех которого, естественно, препятствовал бы нормальной работе приложения.

Затем телефон посылает карте стандартизованные команды. Они обязательно начинаются с заголовка, состоящего из пяти байт. Первый байт (`A0h`) – это класс ISO, присущий SIM-картам. Следующий байт – операционный код команды, и на этом этапе он часто равен `A4h`, что соответствует команде SELECT, используемой для выбора директории или файла с карты. Выбранный адрес занимает два байта,

которые передаются сразу же после повторения картой операционного кода A4h, подтверждающего прием команды (этот байт называется байтом процедуры).

Очень часто телефон начинает с выбора директории 3F00h (это корневая директория SIM-карты). Если считать (вполне закономерно), что эта директория выбирается по умолчанию после сброса, то телефон, скорее всего, сразу же выберет поддиректорию 7F20h (GSM) или 7F21h (DCS), ожидая условий для перехода в директорию 7F10h (Telecom).

После двух байтов отчета (9FXXh), которыми SIM-карта отвечает на любую действительную команду SELECT, почти всегда следует команда GET RESPONSE (C0h), отправленная телефоном. Данная команда требует от SIM-карты передать один или несколько байтов, число которых должно быть равно значению XXh предыдущего отчета. Интерпретация этого ответа позволяет детализировать характеристики директории или выбранного файла: размер, логическую организацию, а также прилагаемые права доступа.

В некоторых случаях команда STATUS (F2h) применяется с той же самой целью или в качестве подтверждения.

Это, в частности, относится к этапу, когда телефон запрашивает, активирован или нет конфиденциальный код карты (сокращенно PIN, или CHV). Если затребовано представление кода, диалог не будет продолжен до тех пор, пока набранный PIN-код не появится на экране. Тогда при помощи команды VERIFY CHV (операционный код 20h) код, набранный на клавиатуре, будет представлен карте, которая ответит 9000h только в одном случае: если код будет признан правильным.

Появление на дисплее команды, начинающейся с A0 10 (Terminal Profile), означает, что SIM-карта совместима с «Фазой 2+» и мобильный телефон поддерживает функции «SIM Toolkit» (STK), перечень которых уточняется в поле «данные» этой команды. Вот, например, результаты, полученные при включении нашей «шпионской» схемы между телефоном RC712 и картой предоплаты (просроченной), PIN-код которой активирован:

```
38 82 00 55 19
A0 A4 00 00 02
A4 7F 20
9F 17
A0 A4 00 00 02
A4 7F 20
9F 17
```

```
A0 A4 00 00 02
A4 7F 20
9F 17
A0 C0 00 00 0E
C0 00 00 00 24 7F 20 02 00 00 44 44 01 09 13 90 00
A0 F2 00 00 14
F2 00 00 00 24 7F 20 02 00 00 44 44 01 09 13 00 14 04 00 83 8A 90 00
```

Совершенно очевидно, что анализ всего диалога, который может составлять тысячи байтов, выходит за рамки данной книги. Книга лишь предлагает средства, благодаря которым вы сами сможете отправиться в увлекательное путешествие, полное приключений.

4.4. ИНТЕРФЕЙСЫ ОБМЕНА ДАННЫМИ

Все мобильные телефоны обычно имеют многоконтактный разъем расширения более или менее универсального назначения. Помимо подключения различных аксессуаров, этот разъем почти всегда позволяет установить последовательное соединение для обмена данными с центральным процессором мобильного телефона. При помощи переходного кабеля для интерфейса RS232 можно обеспечить доступ любого ПК ко всем «секретным» функциям телефона, воспользовавшись информацией и программным обеспечением, свободно полученным из Internet.

Так как существует множество различных моделей телефонов, целесообразным решением была бы разработка универсального модуля, который с одной стороны подключался бы к последовательному порту ПК, а с другой стороны к различным моделям телефонов (с помощью соответствующего соединительного кабеля). Почти недоступный покупателям розничной торговли многоконтактный соединительный разъем, специфический для каждой модели телефона, можно изготовить самостоятельно, разобрав какой-нибудь недорогой аксессуар, например, кабель для автомобильного прикуривателя или комплект hands free для пешехода.

Основной частью всех вариантов схемы подобного модуля является преобразователь уровней (интерфейс) RS232–TTL. В принципе, этот узел является эквивалентом кабелей Minitel, которые были когда-то очень популярны среди электронщиков, увлеченных телематикой.

Несмотря на то что схема, представленная на рис. 4.23, выполнена на широко распространенной микросхеме MAX 232, она имеет некоторые особенности, связанные с данным применением. В отличие от других подобных схем здесь не применяется отдельный источник питания.

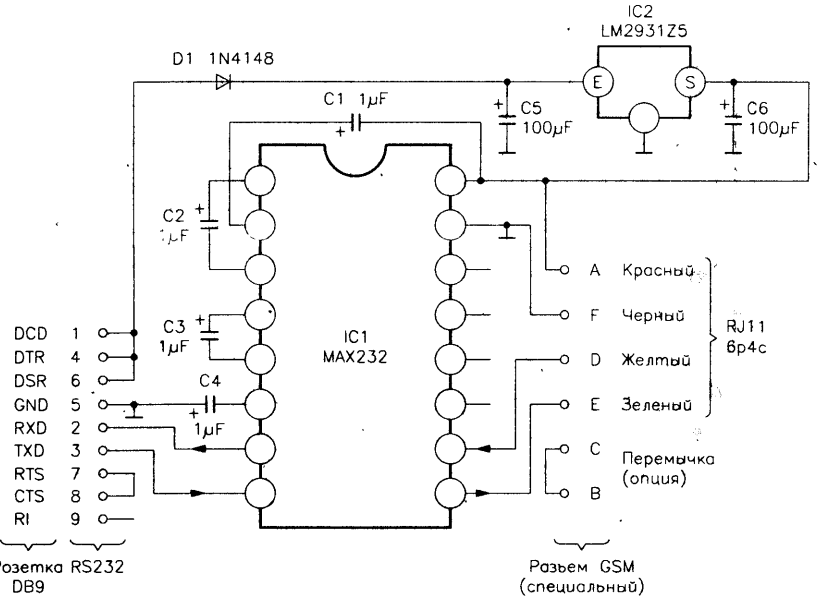


Рис. 4.23. Принципиальная схема интерфейса RS232

Напряжение питания положительной полярности поступает непосредственно из порта RS232 и ограничивается величиной 5 В при помощи стабилизатора, обладающего малыми потерями. Однако в случае большого падения напряжения всегда можно перейти на питание от батарейки напряжением 9 В, которая посоединяется после исключения из схемы диода (в этом случае вместо диода следует установить перемычку). К расположенному на модуле разъему RJ11 (где используются 4 контакта из 6, что обозначается как 6p4c) подсоединяются линии входа и выхода данных, земля и напряжение +5 В, которое необходимо некоторым мобильным телефонам для активирования своего последовательного порта.

Для некоторых моделей требуется также дополнительно соединить, по меньшей мере, два контакта разъема расширения, что удобнее сделать с того конца кабеля, который подключается к разъему RJ11.

Модуль адаптера представляет собой очень простую, небольшую по размерам печатную плату с односторонним монтажом, топология которой показана на рис. 4.24. Перечень элементов к схеме модуля приведен в табл. 4.5.

Собранный в соответствии со схемой размещения элементов, приведенной на рис. 4.25, модуль может подсоединяться либо напрямую

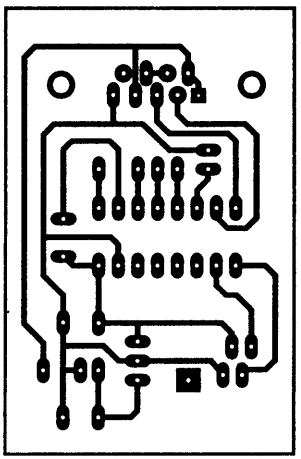


Рис. 4.24. Топология печатной платы модуля интерфейса RS232

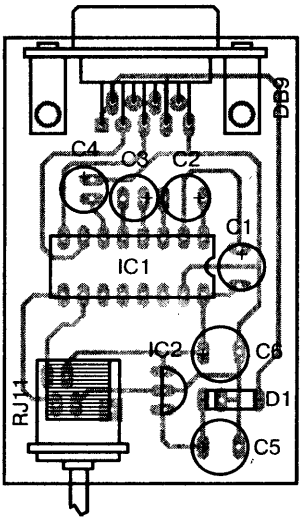


Рис. 4.25. Схема размещения элементов модуля интерфейса RS232

Таблица 4.5. Перечень элементов к рис. 4.25

Наименование	Обозначение	Номинал	Примечание
Конденсаторы	C1 – C4	1 мкФ × 25 В	Вертикальное исполнение
	C5, C6	100 мкФ × 16 В	Вертикальное исполнение
Интегральные микросхемы	IC1	MAX 232	DIP
	IC2	LM 2931 A Z5	
Полупроводники	VD1	1N 4148	
Прочие	Разъем DB9 – розетка		
	Разъем RJ11 (6p4c)		
	Кабель к разъему RJ11		
	Специальный соединительный разъем GSM		
	Элемент питания 9 В и его зажим (опция)		

к порту COM персонального компьютера, либо посредством обычного удлинителя DB9 «вилка-розетка» или переходника DB9–DB25. В качестве специального соединительного кабеля используется многожильный провод от разъема RJ11, или этот разъем монтируется с аналогичным кабелем. Внешний вид собранного модуля интерфейса RS232 приведен на рис. 4.26, а его подсоединение при помощи кабеля к мобильному телефону RC712 – на рис. 4.27.

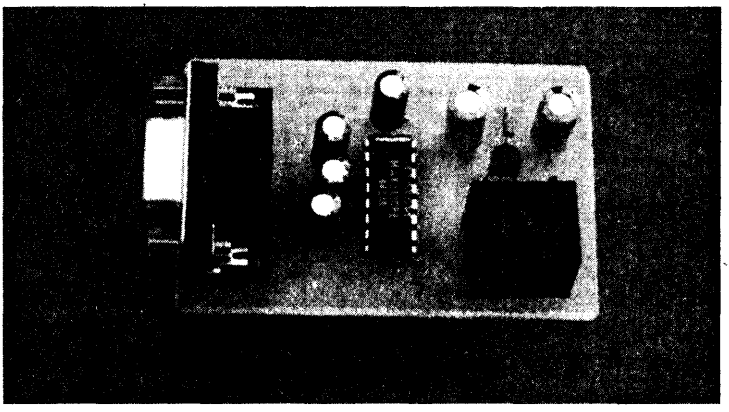


Рис. 4.26. Внешний вид модуля интерфейса RS232

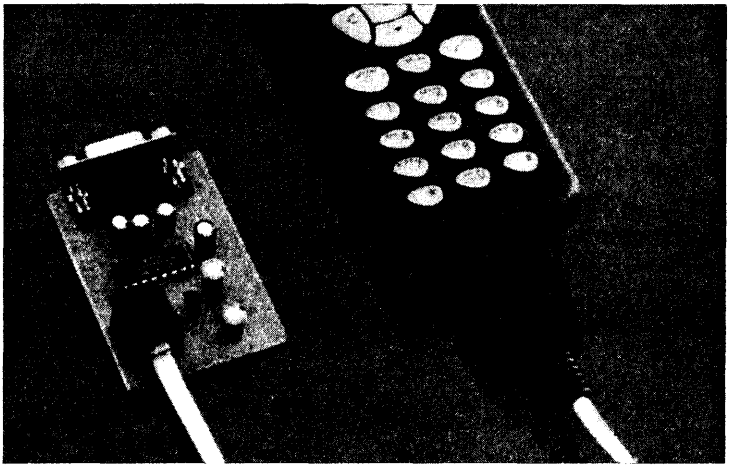


Рис. 4.27. Подключение модуля интерфейса RS232 к мобильному телефону RC712

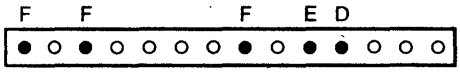
При монтаже следует обратить внимание на правильность использования цвета проводов кабеля: «земля» должна соответствовать черному проводу, а «+5 В» – красному. Ошибки подобного рода могут вызвать пагубные последствия! Затем вам останется смонтировать на другом конце кабеля специальный соединительный разъем, воспользовавшись полученной (например, через Internet) информацией об его цоколевке.

На рис. 4.28 показаны варианты подключения соединительного кабеля к разъемам различных моделей мобильных телефонов. Тут

вы можете действовать по своему усмотрению. Однако, получая из Internet подобную информацию, каждый должен понимать, что использует ее на свой страх и риск.

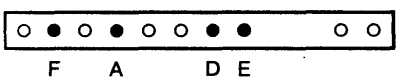
Alcatel one touch (easy, club, max, view)

Со стороны клавиатуры



Alcatel one touch двухдиапазонный (easy, club, max)

Со стороны клавиатуры

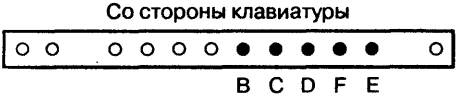


Ericsson 388

Со стороны клавиатуры

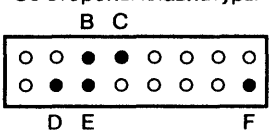
Ericsson 628, 688, 768, 788, 868, 888, A1018s, T10s, T18s, T28s

Со стороны клавиатуры

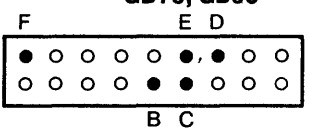


Panasonic G450, G520, G600

Со стороны клавиатуры

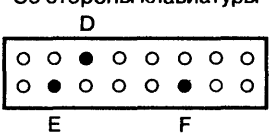


Panasonic GD30, GD50, GD70, GD90



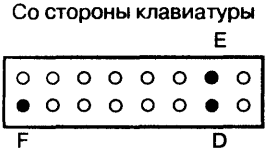
Sagem RC712, 715, 725, 730, 750, 820, 612, 615

Со стороны клавиатуры



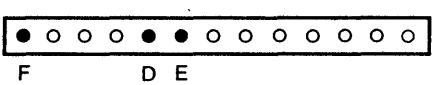
Siemens S6 и S8

Со стороны клавиатуры

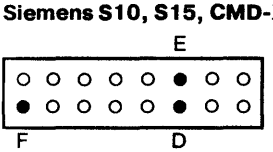


Siemens C25 и S25

Со стороны клавиатуры



Siemens S10, S15, CMD-X2000



Sony CMD-C5

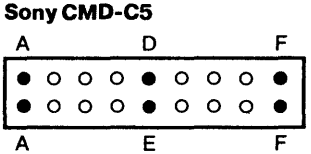


Рис. 4.28. Примеры цоколевки разъемов со стороны телефонов GSM

В принципе, любое коммуникационное ПО (или терминал) под Windows или DOS должно обеспечивать диалог с любым мобильным телефоном, соединенным с ПК при помощи этого устройства. Но подробные описания используемых команд и параметров передачи не всегда доступны. Поэтому очень часто описанная схема используется с программным обеспечением, которое получено из Internet и специально предназначено для выполнения той или иной операции, например для разблокировки мобильного телефона определенной модели. По моему мнению, добрая половина из них работает превосходно, но существуют и программы, способные просто «убить» аппарат.

Следует понимать, что некоторые рискованные команды, посланные на телефон, который находится на гарантии, могут привести к ее потере, а некоторые контракты полностью запрещают любую разблокировку телефона «в обход» специального кода. На мой взгляд, было бы неплохо, если и операторы, со своей стороны, соблюдали бы правила игры и выполняли свои контрактные обязательства, вместо того, чтобы придумывать всевозможные предлоги для их невыполнения.

4.5. ВАРИАНТ ДЛЯ ОДНОПРОВОДНОЙ ШИНЫ

Некоторые мобильные телефоны (в частности, марки Nokia) снабжены разъемом для интерфейса «M2BUS», подключение к которому соответствующего терминала позволяет осуществлять те же самые операции. Поскольку «M2BUS» принадлежит к семейству однопроводных шин (не считая общего провода), требуется применение другой схемы интерфейса.

В схеме, представленной на рис. 4.29, используется микросхема широко применяемой серии CMOS 4000, а именно CD4007. В указанном включении она заменяет обычный инвертор и транзистор с открытым стоком.

Инвертор служит для согласования логических уровней линии RXD интерфейса RS232 и однопроводной шины, обладающей высоким импедансом, тогда как транзистор предназначен для перевода шины в низкое состояние (логический ноль), когда существует положительный уровень на линии TXD RS232.

В режиме ожидания на шине поддерживается высокий уровень при помощи резистора R2, что позволяет как «ведущему» (RS232), так и «ведомому» (мобильному телефону) иметь возможность в любой момент перевести линию на низкий уровень, управляя транзистором микросхемы. Питание микросхемы CD4007 и однопроводной шины осуществляется от последовательного порта и ограничивается до 5 В

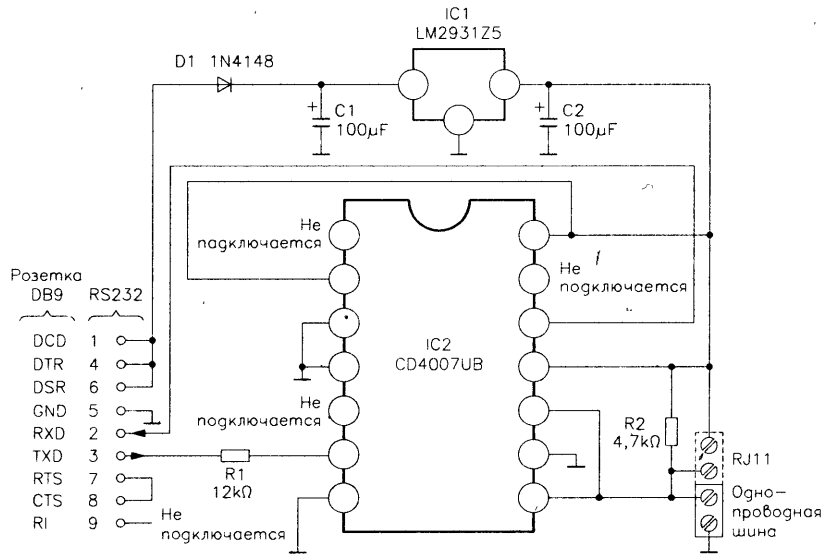


Рис. 4.29. Принципиальная схема интерфейса однопроводной шины

при помощи стабилизатора с малыми потерями, который используется с двумя конденсаторами достаточно большой емкости (100 мкФ).

Эта небольшая схема выполняется на односторонней печатной плате, топология которой приведена на рис. 4.30.

Расположение элементов на печатной плате показано на рис. 4.31. Связь с шиной обеспечивается при помощи разъема RJ11, что также позволяет вывести напряжение + 5 В (на всякий случай). Перечень элементов к схеме приведен в табл. 4.6, а внешний вид собранной платы интерфейса – на рис. 4.32.

На рис. 4.33 показаны два варианта цоколевки разъемов со стороны телефона (действительны для основных моделей Nokia).

На данном этапе легко проверить, правильно ли функционирует интерфейс: когда к шине ничего не подключено, схема соединяет между собой линии TXD и RXD интерфейса RS232. Если плата собрана без ошибок, то при посылке данных в порт COM1 при помощи любого коммуникационного ПО эти же данные и будут приниматься.

4.6. «ПАССИВНЫЙ УСИЛИТЕЛЬ» НА 8 ВТ

Несмотря на то, что большинство существующих сегодня базовых станций рассчитаны на обслуживание мобильных телефонов с выходной

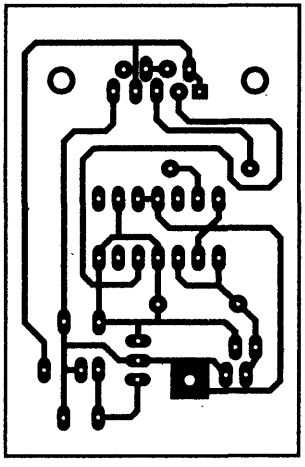


Рис. 4.30. Топология печатной платы интерфейса однопроводной шины

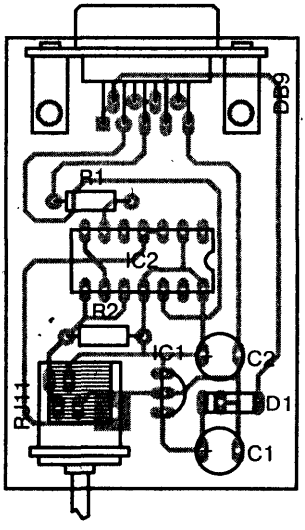


Рис. 4.31. Схема размещения элементов на плате интерфейса однопроводной шины

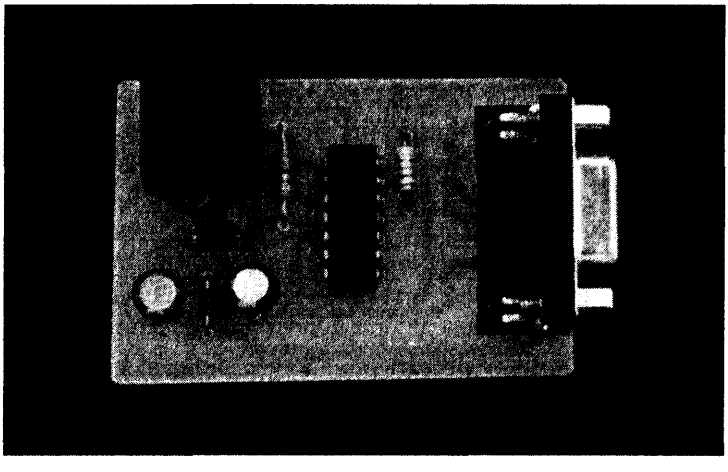


Рис. 4.32. Внешний вид собранной платы интерфейса однопроводной шины

мощностью 2 Вт, в некоторых зонах с недостаточным покрытием могут работать только 8-ваттные телефоны.

А поскольку возможность включения дополнительного усилителя непосредственно между входом телефона и его антенной почти не

Таблица 4.6. Перечень элементов к рис. 4.31

Наименование	Обозначение	Номинал	Примечание
Резисторы	R1	12 кОм	
	R2	4,7 кОм	
Конденсаторы	C1, C2	100 мкФ × 16 В	Вертикальное исполнение
Интегральные микросхемы	IC1	LM 2931A Z5	
	IC2	CD 4007 UB	
Полупроводники	VD1	1N 4148	
Прочие	Разъем DB9 – розетка		
	Разъем RJ11 (6p4c) или другой соединитель		

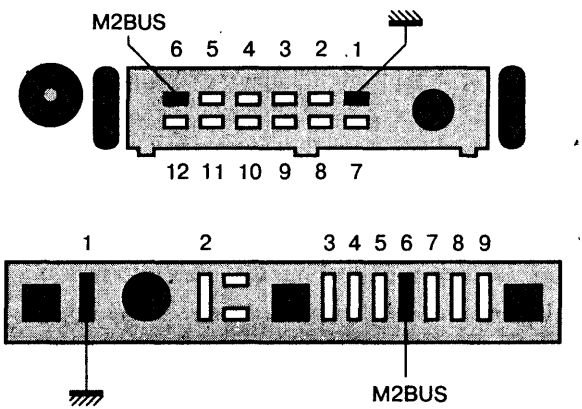


Рис. 4.33. Цоколевка двух вариантов разъемов

рассматривается, можно попытаться существенно изменить диаграмму направленности антенны, чтобы получить подходящий коэффициент усиления, равный 4, хотя бы в направлении основного (максимального) излучения. Естественно, в этом случае предполагается достаточно точная ориентация на базовую станцию и, следовательно, работа в стационарном режиме. Данное условие, как правило, легко выполнимо, так как чаще всего дополнительное усиление сигнала телефона требуется в условиях загородного дома, в кемпинге, в стоящей автомашине и т.д.

Можно даже проводить интересные эксперименты по радиолокации, касающиеся пеленгации и идентификации базовых станций или определения своего местоположения.

На чертеже, приведенном на рис. 4.34, показывается, как можно сконструировать, без каких-либо существенных затрат, пассивный усилитель, представляющий собой не что иное, как антенну типа

«волновой канал». Он, по сути, заменяет антенну 2-ваттного мобильного телефона или подсоединяемую к нему обычную автомобильную антенну.

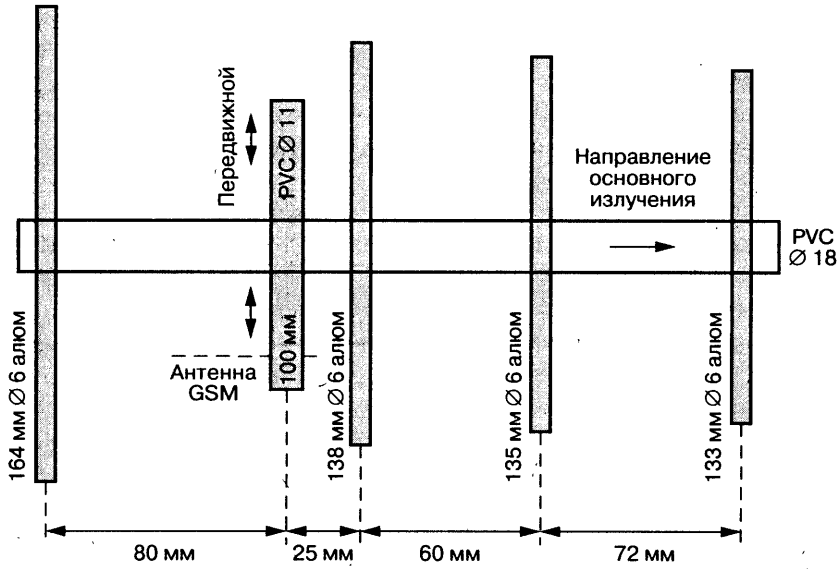


Рис. 4.34. Сборочный чертеж направленной антенны

В направлении максимального излучения коэффициент усиления соответствует приблизительно четырехкратному увеличению эффективности антенны мобильного телефона, что делает его рабочие характеристики сравнимыми с характеристиками 8-ваттного мобильного телефона. Очевидно, что это делается в ущерб усилению по другим направлениям излучения антенны, что, впрочем, помогает ослабить сигналы от нежелательных базовых станций.

Итак, вам понадобятся два куска трубки PVC (из поливинилхлорида), например, могут подойти изоляционные трубки от электрической проводки: одна диаметром 18-20 мм и длиной не менее 26 см, другая диаметром 11 мм и длиной 10 см. Также будут нужны четыре отрезка круглой алюминиевой или медной трубки (сплошной или пустотелой – не имеет значения). Принципиально важным является точное соблюдение (до миллиметра) всех указанных размеров.

В большой пластиковой трубке нужно просверлить пять сквозных отверстий указанных диаметров, а затем плотно вставить в них четыре

металлических элемента и один пластиковый, который должен свободно перемещаться в просверленном отверстии во время настройки. Последующие действия сводятся к тому, что антенна мобильного телефона вставляется в пластиковую трубку диаметром 11 мм таким образом, чтобы основание антенны (в месте ее соединения с корпусом телефона) находилось приблизительно на уровне середины нижнего плеча элемента размером 138 мм. Однако вы можете поэкспериментировать с размещением как самой антенны мобильного телефона, так и элементов «пассивного усилителя». Именно на этом этапе вы оцените приобретенные достоинства своего мобильного телефона, его способность работать в режиме отслеживания trace.

Я не раз убеждался на личном опыте, что только что рассмотренное оригинальное приспособление, просто надетое на антенну обычного 2-ваттного мобильного телефона (см. рис. 4.35) и затем правильно сориентированное, действительно позволяет обеспечивать связь в сети GSM 900 МГц в зонах, считающихся безнадежными. Аналогичное приспособление можно сконструировать и для работы в сети 1800 МГц, предварительно уменьшив размеры элементов пассивного усилителя в 2 раза, но полученные результаты будут менее впечатляющими.

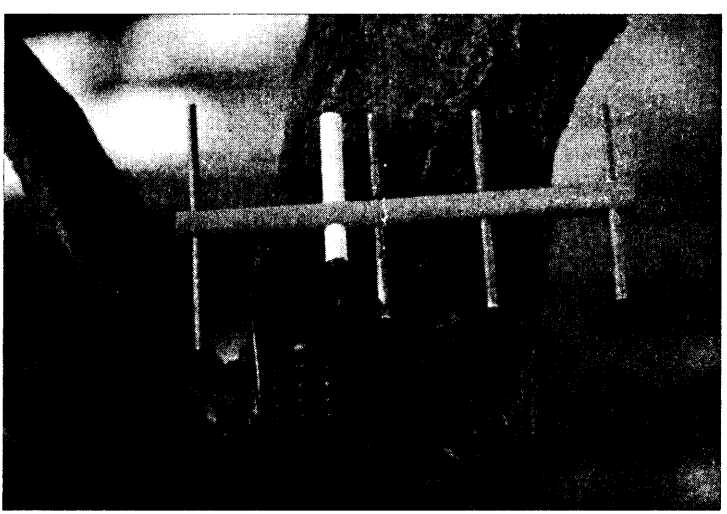


Рис. 4.35. Направленная антенна в рабочем положении. Рекомендуется использовать в режиме hands free или с комплектом пешехода

4.7. SIM-КАРТА ДЛЯ ТЕСТИРОВАНИЯ

Стандарт GSM предусматривает возможность создания так называемых SIM-карт для тестирования, позволяющих проверить все функции мобильного телефона (даже «запертого») без необходимости регистрации в какой-либо сети.

Некоторые производители (например, Motorola) разрешают доступ к скрытым меню только при наличии такой карты.

Обычно SIM-карта для тестирования практически ничем не отличается от карт, выданных оператором, за исключением кода страны (MCC=001), кода сети (MNC=01) и некоторых административных данных, записанных в специальном файле.

К сожалению, совершенно невозможно превратить SIM-карту, у которой закончился срок действия, в карту для тестирования, поскольку соответствующие файлы могут быть изменены только под управлением кода администратора (ADM), ревностно хранимого в секрете каждым дистрибьютором.

Другим решением может стать изготовление имитатора SIM-карты на базе PIC-микроконтроллера, объема памяти которого вполне достаточно для размещения сокращенного набора функций карты для тестирования. Некоторые поставщики предлагают PIC-микроконтроллеры, встроенные в настоящие чип-карты (называемые Wafer Card), которые остается только запрограммировать при помощи соответствующей программы. Речь идет о картах, которые широко применялись для декодирования некоторых платных (закодированных) английских телевизионных каналов. На рис. 4.36 представлена схема такой карты.

Если в вашем распоряжении окажется мобильный телефон, принимающий полноформатные SIM-карты, то самым простым решением будет нанесение рисунка на плату из стеклотекстолита толщиной 0,8/1,0 мм в соответствии с топологией, представленной на рис. 4.37. На данной плате согласно схеме, приведенной на рис. 4.38, будет размещен один единственный компонент – микроконтроллер PIC 16F84 или PIC 16C84.

В Internet распространяются различные общедоступные файлы для программирования PIC-микроконтроллера, при помощи которых он успешно может имитировать различные SIM-карты.

4.8 «BASICSIM» – ИНСТРУМЕНТАЛЬНАЯ SIM-КАРТА

Каждый увлекающийся устройством чип-карт должен быть знаком с BasicCard – удивительным семейством карт, «открытая» операционная система которых программируется на Бейсике (см. http://www.basiccard.com).

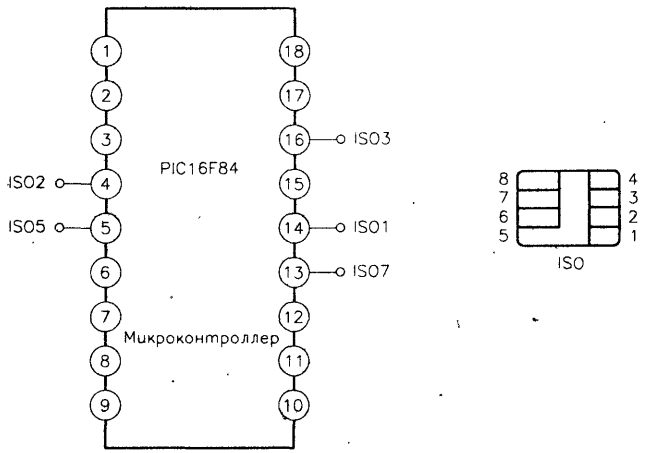


Рис. 4.36. Пример схемы SIM-карты на PIC-микроконтроллере

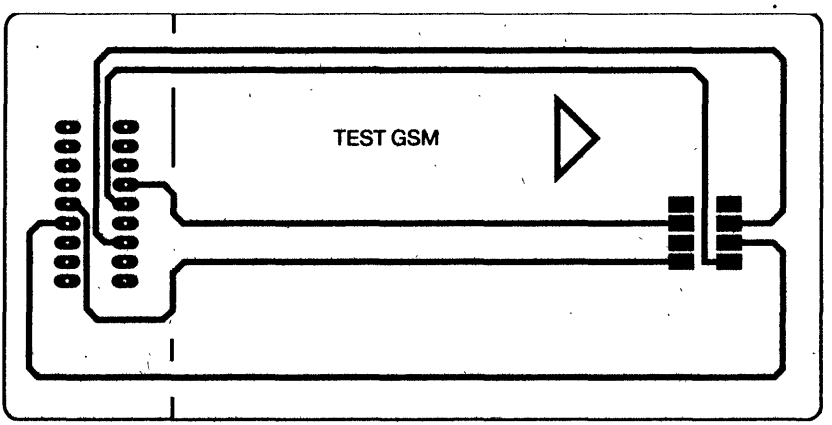


Рис. 4.37. Топология печатной платы имитатора SIM-карты

Прилагаемый к книге компакт-диск содержит различные варианты комплекта для разработки SIM-карт, позволяющие также легко программировать карты, как и при помощи любого считывающего устройства, совместимого с PC/SC (см. главу 5, разработанные мной прикладные программы в версии 3 и совсем новой версии 4).

Таким образом, была придумана BasicSIM, программируемая BasicCard, предназначенная для воспроизведения основных функциональных возможностей SIM-карт (и не только). Например, BasicSIM

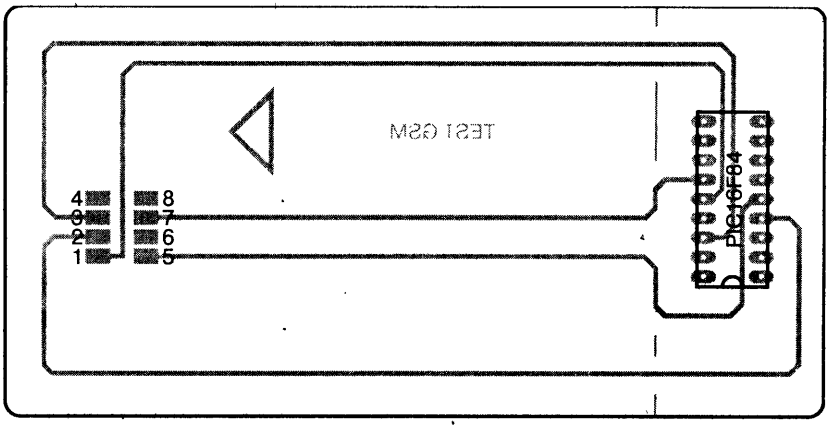


Рис. 4.38. Схема размещения элементов на печатной плате имитатора SIM-карты

приспособлена для записи всех команд GSM 11.11, которые она получает, в открытый файл памяти EEPROM (электронно перепрограммируемая постоянная память). Соответствующая утилита (SIMSPY.EXE) возвращает собранные таким образом данные, перед тем как стереть их для освобождения соответствующего места.

Все программное обеспечение, необходимое для создания и использования BasicSIM, находится в каталоге BASICSIM на компакт-диске и может запускаться даже без установки комплекта BasicCard. Отдельные подкаталоги зарезервированы для каждого варианта BasicCard, который можно преобразовывать в BasicSIM. Здесь вы также найдете несколько пакетных файлов для удобства использования различных считывающих устройств.

Например, для преобразования BasicCard ZC 3.3 в BasicSIM следует войти в папку ZC33. Затем следует выполнить файл MAKEPCSC.BAT, если совместимое считывающее устройство PC/SC подключено к ПК, или MAKECOM2, если считывающее устройство CyberMouse из комплекта BasicCard подключено к последовательному порту COM2, и т.д. Теперь остается инициализировать BasicSIM при помощи утилиты BSUTIL.EXE, которой необходимо послать следующую команду ISO: `C8 06 00 00 00`. Будьте внимательны: отчет о правильном выполнении вернется только через несколько секунд, поэтому не вынимайте карту раньше времени!

Созданная таким образом BasicSIM предоставляет полный доступ ко всем файлам и директориям. Соответственно, различные защитные коды (не только PIN, но и даже ADM!) по желанию можно

дезактивировать. При этом также нейтрализуется всякая возможность блокирования файлов, что позволяет осуществлять манипуляции, которые могут быть ограничены только фантазией экспериментатора (по умолчанию BasicSIM уже сконфигурирована как тест-карта Motorola).

Руководствуясь главой 5 данной книги, вы можете без каких-либо колебаний изменять содержимое того или иного файла в зависимости от предназначения BasicSIM, что собственно и составляет суть увлекательного исследования.

Поскольку карты BasicCard ZC 3.3 и ZC 3.9 используют протокол «T = 1», вопрос об их подключении к мобильному телефону не рассматривается, так как спецификация GSM предусматривает работу по протоколу «T = 0».

Протокол «T = 0» способна поддерживать только «профессиональная» карта BasicCard ZC 4.1 и, следовательно, она может быть признана мобильным телефоном GSM. Эти карты имеются в продаже (http://www.hitechtools.com) и поддерживаются версией 4 комплекта разработки (см. прилагаемый компакт-диск). Версии, базирующиеся на ZC 3.3 или ZC 3.9, предназначены, главным образом, для использования со считывающими устройствами, работающими с программами управления SIM-картами и признающими карты протокола «T = 1». В особенности, это касается устройств для считывания чип-карт CyberMouse, ACR 30, ACR 20, ChipDrive и т.п., которые работают с программами SIMSurf Profi, SIMmate 2000 (если не считать некоторых деталей), а также с разработанным мной программным обеспечением для PC/SC, описанным в главе 5.

Другие программы (PhoneFile, EDSIM 2000 и т.п.), наоборот, отвергают карты протокола «T = 1», начиная сразу с анализа их ответа на сброс (точно так, как это сделала бы настоящая программа GSM), но, естественно, принимают карты версии «T = 0».

Таким образом, можно поэкспериментировать с различными операциями записи и чтения, что обычно невозможно сделать с «настоящими» SIM-картами, оценив соответствующую реакцию того или иного программного обеспечения.

При условии предварительного активирования режима «шпион» на карте BasicSIM (посредством BSUTIL.EXE или команды `C8 A0 00 01 00`) можно будет даже проанализировать содержание диалога, возникшего между BasicSIM и испытываемым программным обеспечением, для чего достаточно запустить исполняемый файл SIMSPY.EXE (аутентичное приложение Windows в графическом режиме) или R.EXE (в консольном режиме).

Следует отметить, что пустая строка в потоке команд указывает на то, что карта подвергалась операции сброса (reset), например, если она вытаскивалась и вставлялась заново.

Два примера подобных диалогов приведены с целью сравнения, а именно: SIMSURF.LOG был записан с помощью карты BasicSIM «T = 1» под управлением программного обеспечения SIMSurf Profi от фирмы Towitoko, а SIMMATE.LOG – после испытания программного обеспечения SIMmate 2000 от фирмы ACS. PH2.LOG и STK.LOG были собраны после установки карты BasicSIM «T = 0» в два телефона GSM:

- RC712 Sagem, совместимый с «Фазой 2»;
- GD90 Panasonic, совместимый с «Фазой 2+» и, значит, с «SIM Toolkit» (STK).

Поскольку байт «Фаза» (7F20:6F7B) BasicSIM был заранее установлен на 03h (Фаза 2+), можно проверить, что второй аппарат передает команду «Terminal Profile» (A0 10 00 00 04 0F 03 FF F7), указывая SIM-карте, что он поддерживает практически весь арсенал функциональных возможностей «SIM Toolkit» и «Proactive SIM» (см. главу 5).

Для манипуляций, не требующих записи диалога в BasicSIM, необходимо дезактивировать эту функцию посредством BSUTIL.EXE или следующей командой ISO:

```
C8 A0 00 00 00
```

Это позволит избежать переполнения памяти карты и ускорит ее работу.

Независимо от работы программного обеспечения SIMSPY.EXE, полезно знать, что BSUTIL.EXE позволяет в любой момент очистить файл (но без сохранения), в котором были записаны команды (команда C8 A2 00 00 00).

В заключение следует отметить, что BasicSIM никоим образом не предназначена для целей аутентичного «клонирования» SIM-карт, поэтому криптографический алгоритм COMP128 на ней не размещен. Вместо него используется элементарный алгоритм манипуляции байтами, который тем не менее позволяет проводить многочисленные эксперименты, связанные с функциями секретности и защиты. В принципе, это решение должно привести к неудаче при любой попытке зарегистрироваться в сети, за исключением, конечно, вызовов срочной помощи путем набора номера 112.

5 SIM-КАРТА

SIM-карта играет в системе GSM совершенно особую и исключительно важную роль. Выпускаемая оператором сети мобильной связи, она фактически осуществляет связь между оператором и клиентом. SIM-карта, установленная в мобильный телефон, предоставляет данные идентификации и аутентификации, необходимые для получения доступа к сети, а затем для шифрования передаваемой информации.

Помимо упомянутой функции, SIM-карта используется для хранения персональных данных, записанных на нее владельцем телефона, начиная с телефонных номеров и заканчивая SMS-сообщениями.

Как и банковская карта, SIM-карта содержит конфиденциальные зоны, доступ к которым должен иметь только оператор, по крайней мере, в том, что касается записи, а также зоны, которые по определению стандарта GSM находятся в распоряжении пользователя.

Тем не менее клиенты имеют все необходимое, чтобы «вмешиваться» в содержимое SIM-карты, несмотря на то что операторы часто относятся к этому крайне отрицательно (что разжигает еще большее любопытство). Чаще всего для получения доступа к содержимому SIM-карты используются меню мобильных телефонов, но, если подключить устройство для считывания чип-карт к микрокомпьютеру, то в своих «исследованиях» можно пойти гораздо дальше.

Целая система конфиденциальных кодов от PIN-кода, защищающего доступ к телефону, до кодов администратора, используемых при выдаче карты, позволяет точно определять права каждой из сторон.

5.1. КОМУ ПРИНАДЛЕЖИТ SIM-КАРТА

Такой вопрос вполне уместен, поскольку некоторые операторы мобильной связи заявляют, что SIM-карты находятся в их собственности, несмотря на то что оплачиваются они клиентами.

Не желая касаться юридических тонкостей, которые выходят за рамки данной книги, имеющей техническую направленность, отметим только, что с трудом можно представить, каким образом операторы могут претендовать на зачисление залоговой суммы на карты, если при возврате карт они воздерживаются от возмещения денег за них. Кроме того, как они могут брать большие деньги за замену потерянной, украденной или поврежденной в процессе «нестандартного» использования карты, помня о том, что клиент, в конце концов, может просто перейти к конкурентам.

Такая «привязанность» операторов к выдаваемым ими SIM-картам говорит о том, что они сами питают сомнения по поводу мер

безопасности, которые принимаются в отношении данных карт, имеющих репутацию столь же надежных, как и банковские карты.

5.2. ЧТО СОДЕРЖИТ SIM-КАРТА

SIM-карта – это нечто большее, чем просто карта с памятью, поскольку ее микропроцессор под управлением операционной системы способен автономно осуществлять обработку информации определенной сложности (в частности, криптографическую).

SIM-карту можно сравнить с дискетой: бóльшая часть содержащейся на ней информации организована в виде древовидной структуры директорий и поддиректорий, принцип построения которой схематически представлен на рис. 5.1.

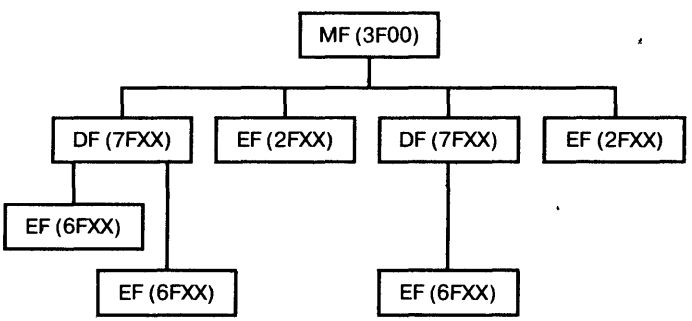


Рис. 5.1. Структура файлов SIM-карты

Команда **SELECT** (операционный код A4h) позволяет свободно перемещаться по рассматриваемой структуре файлов аналогично команде **CD** (Change Directory) в MS DOS.

Корневую директорию, называемую MF (Master File) и имеющую идентификатор 3F00h, можно выбрать с помощью команды ISO:

```
A0 A4 00 00 02 3F 00
```

Следует отметить, что каждый сброс карты (reset) автоматически приводит в эту директорию, поэтому нет необходимости специально ее выбирать.

Корневая директория может содержать несколько так называемых элементарных файлов EF (Elementary Files), идентификатор которых обязательно начинается с 2Fh. Но главное, она включает в себя поддиректории, называемые выделенными файлами DF (Dedicated Files),

идентификатор которых для конкретного случая поддиректории «первого уровня» начинается с 7Fh. В этой поддиректории также размещаются элементарные файлы EF, но их идентификатор начинается с 6Fh.

Стандарт GSM 11.11 дает определение поддиректорий и файлов, наличие которых обязательно (mandatory) и факультативно (optional).

Производители и дистрибьюторы карт свободно могут добавлять собственные директории и файлы к различным уровням этой базовой структуры. Они даже имеют возможность при необходимости размещать на многофункциональной карте дополнительные информационные программы (например, апплеты Java).

Ниже представлен постоянно пополняемый список файлов, обычно содержащихся на недавно выпущенных SIM-картах. Здесь можно встретить исключительно интересные для исследования файлы, о существовании которых большинство пользователей даже и не догадывается.

```
3F00 : Корневая директория
3F00:2F05 (ELP, Extended Language Preference)
3F00:2FE2 (ICCID)
3F00:7F10 Директория «Telecom»
7F10:5F50 (Поддиректория «Graphics»)
7F10:6F3A (ADN, Abbreviated Dialling Numbers)
7F10:6F3B (FDN, Fixed Dialling Numbers)
7F10:6F3C (SMS, Short Messages)
7F10:6F3D (CCP, Capability Configuration Param
7F10:6F40 (MSISDN, Own Numbers)
7F10:6F42 (SMSP, Short Messages Service Parameters)
7F10:6F43 (SMSS, SMS Status)
7F10:6F44 (LND, Last Number Dialed)
7F10:6F49 (SDN, Service Dialling Numbers)
7F10:6F4A (Ext 1)
7F10:6F4B (Ext 2)
7F10:6F4C (Ext 3)
7F10:6F4D (BDN, Barred Dialling Numbers)
7F10:6F4E (Ext 4)
7F10:6F47 (SMSR, Short Message Status Reports)
3F00:7F20 Директория «GSM»
7F20:5F30 (Поддиректория «Iridium»)
7F20:5F31 (Поддиректория «Globalstar»)
7F20:5F32 (Поддиректория «ICO»)
7F20:5F33 (Поддиректория «ACeS»)
7F20:5F40 (Поддиректория «PCS1900»)
7F20:5F60 (Поддиректория «CTS»)
7F20:5F70 (Поддиректория «SoLCA»)
7F20:6F05 (LP, Language Preference)
```

7F20:6F07 (IMSI, International Mobile Subscriber Indentity)
7F20:6F11 (VWMI, Voice Mail Waiting Indicator)
7F20:6F12 (SST, Service String Table)
7F20:6F13 (CFF, Call Forwarding Flags)
7F20:6F14 (ONS, Operator Name String)
7F20:6F15 (CSP, Customer Surface Profile)
7F20:6F16 (CPHS Information)
7F20:6F17 (MBX, VoiceMail Numbers)
7F20:6F20 (Kc, Ciphering Key)
7F20:6F2C (DCK, Depersonalization Control Key)
7F20:6F30 (PLMN, Preferred PLMNs)
7F20:6F31 (HPLMN search period)
7F20:6F32 (CNL, Cooperative Networks List)
7F20:6F37 (ACMM, ACM Maximum value)
7F20:6F38 (SST, SIM Service Table)
7F20:6F39 (ACM, Accumulated Call Meter)
7F20:6F3E (GID1, Group Identifier level 1)
7F20:6F3F (GID2, Group Identifier level 2)
7F20:6F41 (PUCT, Price per Unit and Currency Table)
7F20:6F45 (CBMI, Cell Broadcast Message Identifier selection)
7F20:6F46 (SPN, Service Provider Name)
7F20:6F50 (Call broadcast message identifier range selection)
7F20:6F51 (NIA, Networks Indication of Alerting)
7F20:6F52 (KcGPRS, GPRS Ciphering Key)
7F20:6F53 (LociGPRS, GPRS Location Information)
7F20:6F54 (SUME, SetUpMenu Elements)
7F20:6F74 (BCCH, Broadcast Control Channels)
7F20:6F78 (ACC, Access Control Class)
7F20:6F7B (FPLMN, Forbidden PLMNs)
7F20:6F7E (LOCI, Location Information)
7F20:6FAD (AD, Administrative Data)
7F20:6FAE (Phase)
7F20:6FB1 (Voice Group Call Service)
7F20:6FB2 (Voice Group Call Service Status)
7F20:6FB3 (Voice Broadcast Service)
7F20:6FB4 (Voice Broadcast Service Status)
7F20:6FB5 (eMLPP, enhanced Multi Level Preemption and Priority)
7F20:6FB6 (Automatic Answer for eMLPP Service)
7F20:6FB7 (Emergency Call Codes)

3F00:7F21 Директория "DCS"

(тот же самый перечень, что и 3F00:7F20, для сети DCS 1800)

Описание каждого из этих файлов неизменно дается на английском языке, аббревиатуры, получаемые из названий файлов, являются общепринятыми в системе GSM.

Каждый элементарный файл (EF) может принадлежать одному из трех следующих семейств: прозрачные, линейные и циклические. Он состоит из заголовка (header) и тела (body).

Заголовок детально описывает структуру файла и условия доступа к нему. Его можно прочитать после выбора файла с помощью команды **Get Response** (C0h).

Тело содержит собственно данные, которые могут быть прочитаны с помощью команд **Read Binary** (B0h) и **Read Record** (B2h) и записаны с помощью **Update Binary** (D6h) и **Update Record** (DCh).

Прозрачный файл состоит из определенного числа байтов, доступных по отдельности или блоками, для чего необходимо уточнить их относительный адрес (offset) и длину (length). Первый байт файла, естественно, располагается по относительному адресу 0000h.

Линейный файл состоит из последовательности записей (records) фиксированной длины и в соответствии с этим должен рассматриваться как последовательный. Максимальный объем такого файла составляет 255 записей на 255 байт, не считая расширения.

Проводить запись можно в абсолютном режиме (с уточнением порядкового номера записи), в текущем режиме, в режиме «предыдущий – последующий» или в режиме «первый – последний».

Циклический файл содержит определенное число записей фиксированной длины. При этом каждая новая запись всегда занимает первую позицию, в то время как последняя оказывается «затертой» предпоследней. Отметим, что в такой циклической структуре запись, предшествующая первой, фактически является последней, а запись, следующая за последней – первой.

Подобный тип файла по определению никогда не может оказаться в состоянии перенасыщения, однако существует возможность потери старых данных по мере записи новых.

Прозрачными файлами можно без труда оперировать посредством любого устройства для считывания чип-карт, позволяющего вести прямой диалог через команды ISO (например, используя устройство, изготовленное по схемам, рассмотренным в главе 4).

С линейными и циклическими файлами удобнее работать при помощи специальных программ и промышленных устройств для считывания чип-карт. Такие файлы могут содержать большие объемы информации (например, список из 150 номеров телефонов с соответствующими именами и фамилиями), которыми проще манипулировать в среде базы данных.

Между тем файлы, вызывающие наибольший интерес, практически все принадлежат к типу прозрачных.

5.3. SIM-КАРТА И ИДЕНТИФИКАЦИЯ

Начнем исследование SIM-карты с изучения механизмов ее защиты. В качестве модуля идентификации абонента (Subscriber Identity Module – SIM) SIM-карта хранит в надежном месте регистрационный номер, который идентифицирует своего владельца универсальным для всех стран мира образом. Этот номер может быть прочитан только после представления (или нейтрализации) конфиденциального кода владельца.

Из соображений элементарной осторожности следует воздержаться от передачи в явном виде этого номера по радиоканалам, которые являются чрезвычайно уязвимыми. Несмотря на то что процедуры разработаны таким образом, чтобы максимально избегать подобных случаев, стандарт GSM между тем предусматривает несколько ситуаций, когда разрешается пренебречь упомянутым правилом.

Номер, о котором идет речь, называется международным идентификационным номером мобильного абонента IMSI (International Mobile Subscriber Identity) и представляет собой настоящий номер счета, узнать который можно при помощи конфиденциального кода (PIN или CHV1) владельца. Интересно отметить, что в обычных меню мобильных телефонов его прочтение никогда не предлагается.

Однако прочесть его можно. Идентификационный номер IMSI располагается в файле 6F07 директории 7F20 (GSM), что обычно обозначается как 7F20:6F07.

Как известно, прежде чем получить доступ к данному номеру, необходимо ввести конфиденциальный код, который в рассматриваемом примере имеет вид 1234, а для новой карты это чаще всего 0000 (осторожно, троекратное введение неправильного кода надолго заблокирует карту).

Переведем этот код ASCII в шестнадцатеричный формат и дополним его до восьми цифр (предусмотренный максимум), «набив» FFh. Получится следующий результат:

```
31 32 33 34 FF FF FF FF
```

Для того чтобы представить код карте (после ее ответа на сброс), надо сначала набрать такой заголовок ISO:

```
A0 20 00 01 08
```

Если речь идет об устройстве для считывания, представленном в главе 4, то необходимо дождаться отображения байта процедуры,

отправленного картой (в рассматриваемом случае 20), и затем набрать часть кода, соответствующую собственно данным команды:

```
31 32 33 34 FF FF FF FF
```

При использовании промышленного устройства для считывания байт процедуры фильтруется и можно все набирать за один раз (при этом, однако, исчезает возможность отслеживать приведенный выше диалог).

Если код верный, то в ответ карта отправит 90 00, а если код уже был дезактивирован и карте больше не нужен, то 98 08.

Для того чтобы точно дезактивировать этот код, только создающий неудобства для проводимых экспериментов, можно набрать:

```
A0 26 00 01 08
```

Затем после получения байта процедуры 26 записать:

```
31 32 33 34 FF FF FF FF
```

Код всегда можно снова активировать, если набрать:

```
A0 28 00 01 08
```

После получения байта процедуры 28 следует опять ввести:

```
31 32 33 34 FF FF FF FF
```

Предположим, что код был представлен или дезактивирован, теперь можно приступить к прочтению номера IMSI. Прежде всего следует обратиться к файлу, содержащему необходимую информацию, и очень тщательно выполнить следующие операции:

1. Набрать A0 A4 00 00 02, карта должна ответить байтом процедуры A4.
2. Набрать 7F 20, карта отвечает двумя байтами отчета (в виде 9F XX), которые на данном этапе использоваться не будут.
3. Снова набрать A0 A4 00 00 02, карта выдаст в ответ байт процедуры A4.
4. Набрать 6F 07, карта ответит двумя байтами, на которые не нужно обращать внимания.
5. Набрать A0 B0 00 00 09, и карта, наконец, выдает девять желаемых байт, перед которыми идет байт процедуры B0 и за которыми следует 90 00.

Карта ответит только 98 04, если конфиденциальный код не был представлен или дезактивирован надлежащим образом, и 67 00 при попытке прочитать большее количество байтов, чем содержит номер IMSI.

При использовании промышленного устройства для считывания байт процедуры B0 будет отсутствовать, а отчет 90 00 может отображаться как в начале, так и в конце считываемых данных или отдельно от них и даже совсем не отображаться.

Рассмотрим в качестве вымышленного примера английскую карту. Девять полученных байт могут иметь следующий вид:

```
08 29 43 01 20 20 20 20 20
```

Для того чтобы получить номер IMSI, их надо проинвертировать:

```
809 23410 0202020202
```

Цифры 23410 обозначают английского оператора CELLNET: 234 – код Великобритании (код страны в системе мобильной связи MCC – Mobile Country Code) и 10 – код сети (код сети мобильной связи MNC – Mobile Network Code) ветви мобильной связи British Telecom.

Две цифры, следующие за 23410, называются подмножеством сети (network subset) и могут определять подразделения одной и той же сети (например, относящиеся к различным схемам абонемента или предварительной оплаты, с целью «запирания» отдельных субсидированных телефонов).

Остается, следовательно, восемь цифр для идентификации одной единственной карты из 100 млн потенциальных членов данного подсемейства. А если этого будет недостаточно, то рассматривается вопрос о 15-значном номере IMSI.

Не следует путать международный номер идентификации мобильного абонента IMSI с номером идентификации чип-карты ICCID (Integrated Chip Card IDentification), соответствующим серийному номеру карты, отпечатанному на ней и очень часто на ее упаковке. 10 байт (0Ah), из которых он состоит, не более секретны, чем штрихкод, стоящий на упаковке какого-либо продукта из супермаркета, и могут быть прочитаны, не представляя конфиденциального кода, в файле 2FE2 корневой директории (3F00):

```
A0 A4 00 00 02 2F E2
```

Карта отвечает кодом 9F 0F, который в данном случае следует проигнорировать.

Далее набираем

```
A0 B0 00 00 0A
```

Карта отвечает кодом 90 00, затем отправляет, например, следующие десять байт данных:

```
98 33 01 29 89 20 20 20 20 20
```

После их инвертирования получаем:

```
89 33 10 92 98 02 02 02 02 02
```

Таким образом, данная карта выпущена в 1998 году французским оператором (международный телефонный код страны 33) и имеет серийный номер (естественно, фиктивный) 92 9802 0202 0202.

И наконец, полезно знать, что каждый чип, размещенный на SIM-карте, в свою очередь, идентифицируется с помощью кода ICC, который, например, в картах GemXplore фирмы Gemplus имеет длину 15 байт и записывается в 3F00:0002.

5.4. АУТЕНТИФИКАЦИЯ И ШИФРОВАНИЕ

Как видно из вышеизложенного, идентификационный номер IMSI нельзя считать полностью защищенным от всякого рода «пиратских» действий. Поэтому система безопасности GSM основывается на криптографической аутентификации SIM-карт их дистрибьюторами при помощи секретного алгоритма, называемого A3/A8, или A38.

Одновременно с номером IMSI оператор записывает на SIM-карте секретный ключ (Ki), который также будет храниться в центре аутентификации AuC (Authentification Centre).

Например, для карты GemXplore этот ключ, состоящий из 19 байт, записывается в файлы 7F20:0001 (KeyOp) или 7F20:0011 (KeyMan), где никто, как предполагается, не сможет его считать. Он может использоваться только в самых секретных глубинах карты во время выполнения команды **Run GSM algorithm** (операционный код 88h).

На практике, когда сети необходимо провести аутентификацию SIM-карты мобильного телефона, она генерирует случайное число (RND) из 16 байт (иными словами, 128 бит, откуда и пошло название COMP128 повсеместно используемого алгоритма A3/A8). Центр аутентификации выполняет алгоритм по этому числу RND с ключом, соответствующим идентификационному номеру IMSI SIM-карты, одновременно передавая RND на мобильный телефон.

SIM-карта последнего, со своей стороны, выполняет тот же алгоритм с теми же операндами, что дает следующие результаты:

- подпись (SRES) из 4 байт, которая передается в центр аутентификации с целью сравнения с подписью, рассчитанной в нем самом;
- временный ключ шифрования (Кс) из 8 байт, предназначенный для файла 7F20:6F20 SIM-карты.

Если подписи, вычисленные с одной и другой стороны, идентичны, то сеть признает SIM-карту аутентичной и использует ключ Kc для шифрования поступающей информации при помощи более простого и, следовательно, более быстрого алгоритма. Этот алгоритм, называемый A5, по-видимому, обладает некоторыми недостатками, облегчающими прослушивание разговоров (легальное и нелегальное).

Когда речь заходит о роуминге, то центр аутентификации предоставляет иностранным сетям число RND вместе с соответствующими SRES и Kc, при этом никогда не раскрывая секретного ключа Ki.

Ниже приводится пример использования этого механизма для конкретного образца карты GemXplore, предоставленного компанией Gemplus и снабженного демонстрационным секретным ключом Ki. Случайная величина RND представляет собой эквивалент в шестнадцатеричном формате текста ASCII из 16 знаков слова AUTHENTIFICATION.

Перед выполнением каждого алгоритма необходимо выбрать директорию GSM (7F20):

```
A0 A4 00 00 02 7F 20
```

Карта отвечает, например, $9F_{16}$. Для того чтобы запустить алгоритм GSM, надо набрать:

```
A0 88 00 00 10 41 55 54 48 45 4E 54 49 46 49 43 41 54 49 4F 4E
```

В ответ карта отправляет, например, 9F 0C. Такой отчет говорит о том, что результат содержится в 12 байтах (0Ch). Чтобы с ним ознакомиться, следует применить команду **Get Response** (операционный код C0h) следующим образом:

```
A0 C0 00 00 0C
```

12 байт, инвертированных картой (абстрагируясь от отчета 90 00, свидетельствующего об успехе операции) состоят из подписи SRES (четыре первых байта) и ключа Kc (восемь последних байт). В рассматриваемом примере SRES имеет значение E4 F0 F1 ED. Ключ Kc конфиденциален, поэтому здесь не раскрывается.

Теперь становится понятно, что такой линейный процесс аутентификации, который сеть может периодически осуществлять по мере необходимости, потенциально надежнее, чем системы off-line, используемые, в частности, в области электронных расчетов.

И действительно, права владельцев SIM-карт записаны не на самих SIM-картах, а в базах данных у операторов, где их можно проверить и обновить в режиме реального времени.

5.5. КЛОНИРОВАНИЕ И ПОДДЕЛКА

Как и любая информационная система, обладающая серьезной степенью защиты, система GSM подвергается атакам как со стороны различных мошенников, так и научных работников, имеющих чисто теоретические интересы. Можно констатировать, что плотная завеса секретности более или менее успешно покрывает те области, где, без всякого сомнения, предпочтительнее была бы полная прозрачность.

Всегда лучше проверять систему на прочность перед началом ее массового использования, а не после.

Очевидно, что клонирование карт вполне возможно, хотя и ценой многочасового автоматизированного изучения оригинала. Под клонированием здесь понимается получение идентичного дубликата карты, к которому можно иметь физический доступ. Однако это не имеет большой практической ценности, поскольку можно предположить, что операторы все-таки способны определить записи, которые совпадают на двух картах, имеющих один и тот же идентификационный номер IMEI.

Метод основан на одном из недостатков алгоритма GSM, позволяющего вычислить ключ из результатов, полученных на базе не слишком большого числа проб с подобранными определенным образом величинами RND.

Тем не менее на сегодняшний день кажется невозможным восстановить ключ, исходя из перехваченных, например, через радиоканал данных.

Настоящая подделка состоит в создании всех составляющих пары IMEI/Ki, которая может быть признана действительной хотя бы одной сотой в сети. За исключением серьезных сбоев в системе безопасности той или иной соты в той или иной сети (чего, в принципе, нельзя полностью исключить), «утечки» должны происходить на самом высоком уровне этой системы собственно у оператора.

В реальности самые грубые фальсификации происходят на административном, а не техническом уровне, и осуществляются обычно в контексте межграничного роуминга. Известно, что в своей массе они базируются на выдаче фиктивных абонементов и, следовательно, на использовании настоящих SIM-карт, выпущенных совершенно обычным образом самими операторами.

Необходимо знать, что карта, проданная в комплекте с мобильным телефоном, чаще всего готова к использованию, но доступ к сети предоставляется по ней только после подтверждения соответствующего счета в базе данных оператора.

Другими словами, на данный момент невозможно мгновенно открыть счет клиента без проведения необходимой элементарной предварительной проверки. А это еще один аргумент в пользу схем на базе предварительной оплаты.

5.6. ФАЗЫ РАЗВИТИЯ СТАНДАРТА GSM И ТАБЛИЦА УСЛУГ, ПРЕДОСТАВЛЯЕМЫХ SIM-КАРТОЙ

Спецификация GSM разработана таким образом, что она остается открытой для последующего развития, не отказываясь при этом от предыдущих поколений телефонов и SIM-карт.

Для обеспечения совместимости как с предыдущими (совместимость «назад»), так и с последующими (совместимость «вперед») поколениями мобильных телефонов и карт, не говоря уже о сетях, необходимо, чтобы и телефоны, и карты могли обмениваться друг с другом информацией о своих возможностях.

Основные этапы развития стандарта GSM идентифицируются последовательными фазами. Фаза 1 соответствует упрощенному стандарту GSM в том его виде, который отвечал необходимости запуска еще не до конца разработанной системы (см. главу 1). Фаза 2 относится к более полной системе, которая уже смогла привлечь столь большое число новых пользователей мобильной связи.

На момент написания этой книги фаза 2+ системы GSM является коммерческой реальностью, и все говорит о том, что на этом дело не остановится.

Именно мобильный телефон должен адаптироваться к возможностям карты, считывая в моменты, следующие за включением напряжения, байт фазы SIM-карты. Этот байт, записанный в файле 7F20:6FAE, имеет значение 02 в случае фазы 2 или 03 в случае фазы 2+. Подразумевается, что фаза 1 имеет значение 00 по умолчанию, поскольку само наличие файла «Фаза» обязательно только начиная с фазы 2.

Это один из тех редких файлов, который можно считывать без представления конфиденциального кода, просто выполнив после сброса три следующих команды:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F AE
A0 B0 00 00 01
```

Таким образом можно увидеть, как получается отчет 67 00 (вместо 90 00) при попытке прочитать более одного байта (превышение длины файла).

Если иметь в своем распоряжении образец карты фазы 1, то можно получить, начиная со второй команды, отчет 94 04, говорящий о попытке выбрать файл, который не существует.

Более глубокий анализ возможностей SIM-карты предполагает расшифровку содержимого файла с адресом 7F20:6F38, носящего название «Таблица услуг, предоставляемых SIM-картой» – SST (SIM Service Table).

Основные возможности системы GSM сводятся к некоторому числу услуг, каждая из которых может быть доступной или нет и активированной или дезактивированной.

Список таких услуг остается открытым, что позволяет постоянно разрабатывать новые возможности, не дожидаясь появления новой фазы.

Для каждой SIM-карты существует таблица SST, в которой детально представлены услуги, потенциально поддерживаемые картой, а также указано, активированы они или нет.

Таким образом, оператор мобильной связи может постепенно предлагать новые возможности своим клиентам, просто активируя услуги, которые дожидались своей очереди на карте. При этом необходимости в замене карты может даже и не возникнуть.

В табл. 5.1 показано, как организована подобная таблица SST, где каждый байт соответствует четырем услугам.

Понятно, что длина этого файла может меняться от одной SIM-карты к другой, и он будет тем длиннее, чем современнее и мощнее карта.

Считывание таблицы SST требует предварительного представления (или, что более удобно, дезактивирования) кода PIN (CHV1), а запись – кода администратора ADM1.

Таблица 5.1. Структура таблицы услуг, поддерживаемых SIM-картой (7F20:6F38)

Байт	Активирование	Наличие	Услуги GSM
1	b2	b1	Услуга 1 : Отключение функции CHV1 (PIN1)
	b4	b3	Услуга 2 : Ускоренный набор номера (ADN)
	b6	b5	Услуга 3 : Набор фиксированных номеров (FDN)
	b8	b7	Услуга 4 : Хранение коротких сообщений (SMS)
2	b2	b1	Услуга 5 : Извещение о стоимости разговоров (AoC)
	b4	b3	Услуга 6 : Возможность конфигурации параметров (CCP)
	b6	b5	Услуга 7 : Выбор PLMN
	b8	b7	Услуга 8 : Подадрес стороны
3	b2	b1	Услуга 9 : MSISDN
	b4	b3	Услуга 10 : Расширение 1
	b6	b5	Услуга 11 : Расширение 2
	b8	b7	Услуга 12 : Параметры SMS
4	b2	b1	Услуга 13 : Последний набранный номер (LND)
	b4	b3	Услуга 14 : Идентификация соты, передающей сообщение
	b6	b5	Услуга 15 : 1-й уровень группы идентификации
	b8	b7	Услуга 16 : 2-й уровень группы идентификации

Таблица 5.1. Структура таблицы услуг, поддерживаемых SIM-картой (7F20:6F38) (окончание)

Байт	Активирование	Наличие	Услуги GSM
5	b2	b1	Услуга 17 : Наименование службы провайдера
	b4	b3	Услуга 18 : Служба набора номеров (SDN)
	b6	b5	Услуга 19 : Расширение 3
	b8	b7	Услуга 20 : RFU
6	b2	b1	Услуга 21 : Список идентификаторов группы VCGS (EF VGCS и EF VGCSS)
	b4	b3	Услуга 22 : Список идентификаторов группы VBS (EF VBS и EF VBSS)
	b6	b5	Услуга 23 : Услуга расширенного многоуровневого приоритета и прерывания обслуживания eMLPP
	b8	b7	Услуга 24 : Автоматический ответ для eMLPP
7	b2	b1	Услуга 25 : Загрузка данных через SMS-CB
	b4	b3	Услуга 26 : Загрузка данных через SMS-PP
	b6	b5	Услуга 27 : Выбор меню
	b8	b7	Услуга 28 : Управление вызовом
8	b2	b1	Услуга 29 : Proactive SIM
	b4	b3	Услуга 30 : Диапазоны идентификации соты, передающей сообщение
	b6	b5	Услуга 31 : Запрет набора номеров (BDN)
	b8	b7	Услуга 32 : Расширение 4
9	b2	b1	Услуга 33 : Деперсонализация управляющих ключей
	b4	b3	Услуга 34 : Список объединенных сетей
	b6	b5	Услуга 35 : Отчеты о статусе коротких сообщений
	b8	b7	Услуга 36 : Индикация в сети об аварийной ситуации на мобильной станции (MS)
10	b2	b1	Услуга 37 : Управление короткими сообщениями, исходящими от мобильной станции, при помощи SIM-карты
	b4	b3	Услуга 38 : GPRS
	b6	b5	Услуга 39 : Изображение (IMG)
	b8	b7	Услуга 40 : Поддержка услуг местной сети (SoLSA)
11	b2	b1	Услуга 41 : USSD-объект строковых данных, поддерживаемый в управлении вызовом
	b4	b3	Услуга 42 : Команда RUN AT COMMAND

Примечание к таблице:

1. b – обозначает определенный разряд в соответствующем байте:
   b8 = 128 b6 = 32 b4 = 8 b2 = 2
   b7 = 64 b5 = 16 b3 = 4 b1 = 1
2. RFU (Reserved for Future Use) – зарезервировано для будущего использования

Когда это сделано, с помощью двух следующих команд выбирают таблицу:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 38
```

Например, для того чтобы прочитать пять первых байт (но их может быть и больше), нужно набрать:

```
A0 B0 00 00 05
```

В каждом байте каждая услуга соответствует двум битам, принимающим следующие значения:

- 00 – услуга отсутствует и, естественно, не действует;
- 01 – услуга имеется на карте, но не действует;
- 11 – услуга активирована и, естественно, имеется на карте.

Сочетание 10 явно неправомерно, поскольку оно подразумевает активирование несуществующей услуги.

На рис. 5.2 подробно представлено содержимое двух карт с предварительной оплатой, выпущенные оператором 208–01 в 1998 и 1999 году соответственно.

Считывая пятый байт каждой из карт, можно заметить, что услуга 18 (номера услуг) была добавлена и активирована в промежуток времени, разделяющий выпуск обеих карт. Это позволяет проследить эволюцию возможностей мобильных телефонов, где более поздние модели предлагают отдельное меню для номеров специальных услуг, которые не могут быть изменены владельцем (служба сообщений, служба клиентов и т.д.).

Конечно, для практического использования этой возможности необходимо, чтобы она поддерживалась мобильным телефоном. Например, именно так и будет, если карту, выпущенную совсем недавно, вставить в телефон модели «MCT Vibreur» фирмы Sagem, но не предыдущей версии (где вибратор отсутствует) того же самого мобильного.

И наоборот, если вставить карту давнего срока выпуска в мобильный телефон самой последней модели, то соответствующее меню SERVices OPERateur

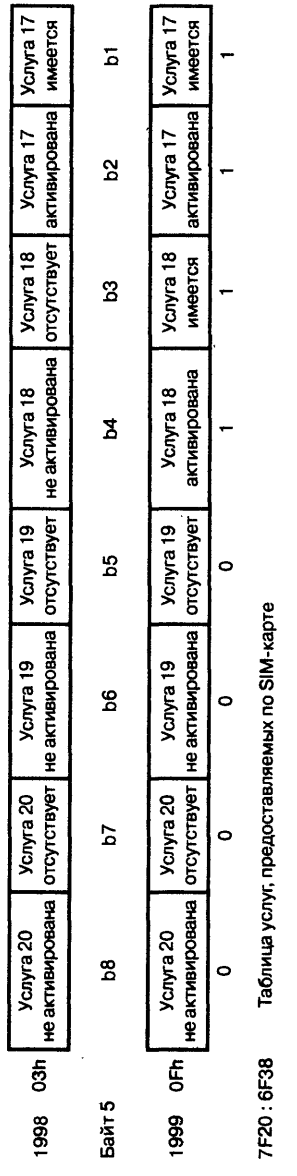


Рис. 5.2. Сравнение возможностей двух карт с предварительной оплатой (оператор 208–01)

(Услуги операторов) останется в скрытом виде, поскольку из таблицы SST телефону сообщается, что данная карта не поддерживает соответствующую услугу.

Таким образом, вы можете поупражняться в обнаружении различий, существующих между картами, таблицы услуг SST которых содержат следующее:

- оператор 208–10, год выпуска 1998: `DF 3D DF 5F 3D`;
- оператор 208–10, год выпуска 1999: `FF 3C FF 7F 3D`;
- оператор 228–01, год выпуска 1999: `FF 3F FF FF 03`.

Другим исключительно интересным примером является карта немецкого оператора 262–02, взятая из демонстрационной версии программы SIMSurf, находящейся на компакт-диске.

Декодирование первого байта ее таблицы услуг SST (`FD 3F FF 0F`) показывает, что услуга 1 (отключение PIN-кода) не активирована. Иными словами, это означает, что пользователь не может отказаться от той степени защиты (иногда излишней), которую ему гарантирует обязательное представление его конфиденциального кода при каждом включении мобильного.

Только оператор, выдавший карту, может под контролем кода администратора ADM1 изменить таблицу услуг SST таким образом, чтобы разблокировать эту возможность.

Естественно, нет смысла обсуждать здесь каждую из услуг SST, но тем не менее некоторые из них заслуживают подробного рассмотрения.

Так, например, услуга 15 связана с наличием на SIM-карте файла под названием GID1 (`7F20:6F3E`). Он служит в основном для «запирания» (SIMlocking – блокировка подключения другой SIM-карты) некоторых субсидированных мобильных телефонов. Это относится не к отдельной SIM-карте (идентифицированной ее номером IMSI), а к семейству SIM (имеются в виду некоторые серии карт с предварительной оплатой, которые выпускаются конкретным оператором).

Поэтому в файле GID1 на определенных картах с предварительной оплатой, выпускаемых оператором 208–01, можно встретить эквивалент текста ASCII «MO01» или «MO02» в шестнадцатеричном формате.

Поскольку число байтов GID1 (также как и GID2) строго не определено, воспользуемся возможностью, возникающей при его считывании, чтобы слегка коснуться (так как это довольно сложно) вопроса заголовков файлов.

До сих пор не рассматривался отчет, отправляемый последней командой **SELECT** и предназначенный для отбора представляющего интерес файла.

Рис. 5.3. Расшифровка заголовка файла

Так как всегда предполагается, что код CHV1 представлен или нейтрализован (дезактивирован), начнем с выбора файла GID1:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 3E
```

Если файл 7F20:6F3E на карте отсутствует (и это не редкость), то мы получим отчет 94 04 (файл не существует).

Предположим, что результатом этого действия будет отчет 9F 0F, означающий, что 15 (0Fh) байт заголовка могут быть считаны при помощи команды **Get Response** (операционный код C0). Поэтому перед любой другой командой (это важно) необходимо выполнить:

```
A0 C0 00 00 0F
```

Например, при использовании упоминавшейся выше карты (оператора 208–10) 1998 года выпуска можно получить в сопровождении отчета 90 00 следующий ответ:

```
00 00 00 03 6F 3E 04 00 14 FF 44 01 01 00 00
```

Рис. 5.3 поможет расшифровать его содержание. Поскольку речь идет о файле типа EF, сразу можно увидеть, что получение в ответ 15-ти байт вполне нормально. В байтах 5 и 6 (IDENT) находится идентификатор рассматриваемого файла (6F 3E для GID1).

Байты с 1 по 4 (SIZE, размер) указывают общее число байтов файла (в данном случае 3), в то время как байт 14 показывает, что дело касается «прозрачного» файла (самый простой случай).

В случае, например, линейного файла, байт 15 уточняет длину (LENGTH) каждой записи, что позволит вычислить число всех записей путем простого деления SIZE/LENGTH (размер/длина).

Байт 7 (TYPE, тип) подтверждает, что речь действительно идет о файле EF. Оставшаяся часть ответа карты уточняет условия доступа и состояние файла (правомочный или недействительный). Эти детали еще более сложны и обеспечиваются программами, специализирующимися на работе с SIM-картами.

Именно таким образом можно, в частности, узнать, каким кодам подчинено считывание и/или запись в файле, но еще проще сделать собственные пробы.

В свете того, о чем было только что сказано, можно без колебаний приступить к прочтению трех байт, расположенных в GID1:

```
A0 B0 00 00 03
```

Полученный ответ (FF FF FF) дает основания думать, что мобильный телефон, проданный с этой картой, был закодирован не файлом GID1. Это предположение может быть проверено, если вставить в телефон другую карту того же типа, которая действительно будет отторгнута.

Выяснилось, что рассматриваемая карта MO01, напротив, может быть использована в мобильном телефоне, проданном с картой MO02, при этом кода «отпирания» не требуется, так как разные операторы вряд ли могут применять сильно отличающиеся варианты кодирования.

Само наличие некоторых услуг SST возможно только в том случае, если карта соответствует фазе 2+ (03h), поддерживает «SIM Toolkit» (STK) или является картой «Proactive SIM».

При выполнении указанных условий SIM-карта распознает команду «Terminal Profile», которая, в свою очередь, может быть послана только мобильным телефоном, совместимым с «Фазой 2+». В противном случае SIM-карта возвратит отчет 6D00, сообщающий о том, что команда неизвестна.

Указанная команда, обычно выполняемая один единственный раз при инициализации телефона, имеет формат A0 10 00 00 LEN и содержит поле данных, длина которого (LEN) зависит от степени «продвинутости» телефона. Каждый бит поля данных соответствует конкретной функции, которую мобильный телефон может (бит установлен в 1) или не может (бит установлен в 0) выполнить по запросу SIM-карты:

```
Байт 1 :
Бит 1 : Загрузка Profile
Бит 2 : Загрузка данных SMS-PP
Бит 3 : Загрузка данных, передаваемых сотой
Бит 4 : Выбор меню
```

```
Байт 2 :
Бит 1 : Результат выполнения команды
Бит 2 : Управление вызовом при помощи SIM-карты

Байт 3 (Proactive SIM):
Бит 1 : Текст дисплея
Бит 2 : Получить Inkey
Бит 3 : Получить вход в сеть
Бит 4 : Дополнительное время
Бит 5 : Воспроизведение тональности
Бит 6 : Опрос интервала
Бит 7 : Выключение опроса
Бит 8 : Обновление

Байт 4 (Proactive SIM) :
Бит 1 : Выбор строки
Бит 2 : Послать короткое сообщение
Бит 3 : Послать SS
Бит 4 : Послать USSD
Бит 5 : Настройка вызова
Бит 6 : Настройка меню
Бит 7 : Предоставить местную информацию
```

(Биты, не указанные в списке, зарезервированы для использования в будущем).

В качестве упражнения попытайтесь декодировать «Terminal Profile» (`0F 03 FF F7`), находящийся в файле STK.LOG, который содержится в каталоге BASICSIM на прилагаемом компакт-диске.

В главе 4 было описано, каким образом этот файл можно записать на SIM-карту из комплекта «BasicSIM», вставленную в мобильный телефон, совместимый с «Фазой 2+».

Отдельно следует отметить, что функция «Послать USSD» необходима для использования некоторых дополнительных функциональных возможностей (например, отправки SMS) карты GSM CARD easyRoam, описанной в главе 2.

В некоторых последних моделях мобильных телефонов биты, ранее зарезервированные для использования в будущем («RFU»), в настоящее время начинают устанавливаться в «1».

5.7. ПРЕДВАРИТЕЛЬНЫЙ ВЫБОР ЯЗЫКА

Как правило, меню мобильных телефонов предлагают опцию, позволяющую выбрать, на каком языке будет отображаться информация на дисплее.

Если этот выбор не делается по умолчанию (автоматический режим), то телефон может учитывать предпочтения, зафиксированные в SIM-карте (оператором или пользователем).

Таким образом, текст будет автоматически воспроизводиться на соответствующем языке, если владелец вставит SIM-карту в телефон, установленный во взятом напрокат автомобиле или в такси. Такая функция независимо от таблицы услуг SST обращается к файлу «предпочитаемый язык» LP (Language Preference), расположенный по адресу 7F20:6F05. В нем можно записать код одного единственного или нескольких языков в порядке убывания приоритета, руководствуясь следующими принятыми обозначениями:

- 00 – немецкий;
- 01 – английский;
- 02 – итальянский;
- 03 – французский;
- 04 – испанский;
- FF – предпочтения нет.

Например, в соответствующем файле международной карты GSM CARD easyRoam можно прочитать код 01 00 03 04, выполнив следующие команды:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 05
A0 B0 00 00 04
```

Для того чтобы на любой карте, поддерживающей такую функцию, выбрать в качестве приоритетного французский язык, необходимо воспользоваться (после представления или дезактивации конфиденциального кода CHV1) следующей последовательностью команд:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 05
A0 D6 00 00 01 03
```

Начиная с «Фазы 2+», в корневом каталоге SIM-карт может находиться файл, называемый ELP (Extended Language Preference, расширенные языковые предпочтения). В телефонах, совместимых с последними стандартами, данный файл имеет более высокий приоритет, чем файл LP. В этом случае изменения, производимые в файле LP, не принесут никакого результата.

5.8. КЛАССЫ ДОСТУПА

Всем известно, с какой легкостью в сети GSM возникает режим локальной перегрузки, когда обстоятельства заставляют большое количество людей одновременно пользоваться своими мобильными телефонами.

Во избежание тотальной блокировки, в том числе номеров службы спасения и службы безопасности, поскольку эти службы также оснащены телефонами GSM, было решено создать классы приоритета, распределяемые случайным образом. Однако возникает подозрение, что определенные категории наиболее «рентабельных» абонентов обладают в этом смысле некоторыми преимуществами.

В стандарте GSM 02.11 дается определение десяти обычных классов доступа, имеющих номера с 0 до 9, и пяти специальных классов – с 11 по 15:

- 11 – зарезервировано за сетью;
- 12 – службы безопасности;
- 13 – общественные службы (вода, газ и т.д.);
- 14 – службы срочной помощи;
- 15 – персонал оператора.

Класс под номером 10 играет особую роль, поскольку по умолчанию к нему относятся все мобильные телефоны. Он управляет прохождением вызовов срочной помощи (в частности, по номеру 112).

Телефон обычного клиента относится к одному единственному классу от 0 до 9, в то время как абонент специального класса, может, помимо этого, принадлежать еще и обычному.

Использование мобильного телефона в конкретной соте возможно только в том случае, если в данной местности, по крайней мере, один из его классов имеет на то разрешение от сети.

Иными словами, это означает, что в ситуации опасности класс 10 может быть заблокирован, что сделает невозможными вызовы срочной помощи в данном месте, в то время как некоторые привилегированные клиенты смогут использовать свои мобильные телефоны как обычно.

С точки зрения функциональности эти меры вполне понятны, но о них также должны быть осведомлены и владельцы мобильных телефонов, от которых, как правило, эта информация скрывается. Упомянутые меры могут привести к тому, что из соображений безопасности люди начнут обзаводиться несколькими телефонами (или SIM-картами) от конкурирующих операторов или, что еще лучше,

одной единственной картой от зарубежного оператора, предлагающего широкие возможности роуминга.

Рассматриваемые классы, защищенные конфиденциальным кодом пользователя, можно найти в файле 7F20:6F78 (ACC) при помощи следующей последовательности команд:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 78
A0 B0 00 00 02
```

Результатом такого считывания будут два байта, закодированные приведенным ниже образом, где бит определяет свойства каждого класса (исключением является бит, который соответствует классу 10 и всегда равен 0):

- 00 01 – класс 0;
- 00 02 – класс 1;
- 00 04 – класс 2;
- 00 08 – класс 3;
- 00 10 – класс 4;
- 00 20 – класс 5;
- 00 40 – класс 6;
- 00 80 – класс 7;
- 01 00 – класс 8;
- 02 00 – класс 9;
- 08 00 – класс 11;
- 10 00 – класс 12;
- 20 00 – класс 13;
- 40 00 – класс 14;
- 80 00 – класс 15.

Из этого следует, что одновременная принадлежность нескольким классам сводится к простому сложению соответствующих величин (например, F8 01 для класса 0 и всех классов приоритета, сочетание которых позволяет почти во всех обстоятельствах вызвать срочную помощь).

5.9. УПРАВЛЕНИЕ СЕТЯМИ

Два файла – FPLMN с адресом 7F20:6F7B и PLMN с адресом 7F20:6F30 – содержат, соответственно, списки запрещенных (forbidden) и предпочтительных сетей PLMN (Public Land Mobile Networks – наземная сеть мобильной связи общего пользования). Оба списка защищены как от считывания, так и от записи только конфиденциальным кодом

пользователя (CHV1), следовательно, владелец телефона может свободно ими манипулировать.

Ознакомление с содержимым файла FPLMN позволяет узнать, запрещены ли оператором, выпустившим карту, попытки регистрации в сетях конкурентов, или много ли данный мобильный телефон уже потерпел неудач при подобной попытке.

Поскольку код сети занимает 3 байта, то 12 байт файла FPLMN позволяют запретить регистрацию только в четырех сетях одновременно.

Считывание файла в полном объеме можно произвести после представления или нейтрализации конфиденциального кода CHV1 с помощью следующей последовательности команд:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 7B
A0 B0 00 00 0C
```

Если взять в качестве примера выданную оператором SIM-карту, то результат будет иметь следующий вид:

```
02 F8 10 02 F8 01 02 F8 02 02 F6 10
```

После инвертирования вышеприведенных байтов получаем:

```
20 8F 01 20 8F 10 20 8F 20 20 6F 01
```

Теперь, не обращая внимания на разграничители F, можно определить коды четырех следующих операторов:

- 208–01 (Orange);
- 208–10 (SFR);
- 208–20 (Bouygues);
- 206–01 (Belgacom).

Вполне возможно отменить (как правило, эфемерным образом) тот или иной запрет, «забив» соответствующий код при помощи FF FF FF. В рассматриваемом примере, для того чтобы снять запрет, касающийся оператора 208–10, достаточно просто ввести следующую команду при условии, что файл FPLMN остается постоянно выбранным:

```
A0 D6 00 03 03 FF FF FF
```

Отметим, что параметры P1 и P2 команды ISO, часто имеющие значение 00 00, в данном случае определяют смещение (03h), которое указывает на четвертый байт файла.

С тем же успехом можно полностью стереть файл FPLMN при помощи следующей команды:

```
A0 D6 00 00 0C FF FF FF FF FF FF FF FF FF FF FF FF
```

Практически таким же образом можно работать с файлом PLMN, содержащим список сетей, с которыми, по желанию оператора (или пользователя), мобильный телефон должен попытаться соединиться в первую очередь. Основное отличие от предыдущего случая заключается в том, что этот список более длинный (часто 10 позиций, то есть 30 байт).

Например, для того чтобы прочитать коды двух первых предпочтительных сетей (то есть 6 байт), нужно сделать следующее:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 30
A0 B0 00 00 06
```

В данном случае операции записи, применяющие операционный код D6, дают возможность пользователю изменить предпочтения, запрограммированные «по умолчанию» оператором в силу его коммерческих интересов.

5.10. ЛОКАЛИЗАЦИЯ МОБИЛЬНОГО ТЕЛЕФОНА

В настоящее время уже предлагаются платные услуги локализации, позволяющие владельцу мобильного телефона определить свое географическое местоположение (в некоторой степени аналогично глобальной системе определения местоположения GPS). Но речь в данном разделе пойдет о другом – об исследовании той зоны SIM-карты, которая позволяет «отслеживать» все перемещения мобильного телефона: LOCI (7F20:6F7E).

Данный файл прозрачного типа длиной 11 байт (0Bh), считывание и запись в котором защищены только конфиденциальным кодом пользователя CHV1, позволяет проводить интересные манипуляции, связанные непосредственно с сетью. Отправив карте приведенную ниже последовательность команд, можно полностью прочитать содержимое рассматриваемого файла LOCI:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 7E
A0 B0 00 00 0B
```

Чтобы извлечь максимум информации из этого блока, состоящего из 11 байт, его надо разбить в соответствии с указаниями, приведенными на рис. 5.4.

Группа из первых четырех байт называется временным идентификатором мобильного абонента TMSI (Temporary Mobile Subscriber Identity). Этот идентификатор присваивается сетью каждому мобильному

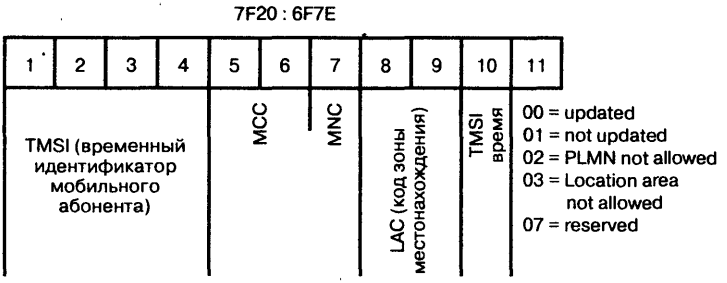


Рис. 5.4. Значения 11 байт файла LOCI

телефону, успешно прошедшему регистрацию, и временно заменяет международный номер IMSI, пока это не вносит сомнений по поводу точной идентификации SIM-карты. При отсутствии регистрации эта зона имеет вид FF FF FF FF.

Байты 5, 6 и 7 содержат полный код (код страны MCC и код сети MNC) последней сети, в которой мобильный телефон успешно зарегистрировался, и сохраняют свое значение вплоть до следующей попытки регистрации. Часто при повторном включении мобильный телефон старается зарегистрироваться прежде всего в этой сети, что побуждает операторов при выдаче карты переписывать в данном файле свой собственный код.

Байты 8 и 9 составляют так называемый код зоны местонахождения LAC (Location Area Code), то есть идентификатор последней географической зоны, в которой мобильный был отмечен. Как правило, эта зона достаточно обширна и включает значительное число сот одного и того же оператора.

Байт 10 (TMSI time, время) практически бесполезен в случае фазы 2, в то время как байт 11 описывает последнюю ситуацию, в которой находился мобильный по отношению к сети:

- 00 – наиболее распространенная ситуация, когда регистрация мобильного телефона была своевременно обновлена (updated) в последней соте его пребывания;
- 01 – (not updated – регистрация не обновлена) может встретиться на новых картах или как следствие неудачной регистрации;
- 02 – (PLMN not allowed) и 03 – (Location area not allowed) информируют о том, что регистрация мобильного телефона не была разрешена, соответственно, либо в последней запрашиваемой сети, либо в последней зоне посещения;
- 07 – (reserved) резервный.

Например, на карте, которая использовалась обычным образом, можно прочитать следующее:

```
2A F6 AB 6E 02 F8 01 12 C1 1E 00
```

Карта, которой было отказано в регистрации в конкурирующей сети, может содержать:

```
FF FF FF FF 02 F8 01 FF FE 14 01
```

А просроченная карта может выдать следующее:

```
FF FF FF FF 02 F8 01 FF FE 00 03
```

Здесь автор предоставляет читателям возможность самим постараться восстановить, что же произошло на самом деле, с каким оператором и в каком регионе. Чтобы провести несколько занимательных экспериментов, воспользуйтесь возможностью записи в файл LOCI, как ни странно, предоставленной пользователю.

«Забивка» файла LOCI карты оператора файлом, считанным на карте конкурента, часто приводит к тому, что на протяжении нескольких мгновений мобильный телефон воспроизводит имя сети, в которой обычно ему регистрироваться запрещено. Кроме того, если стереть список запрещенных сетей (FPLMN) и таким образом присвоить последнему байту значение 00, то это может привести к весьма интересным результатам.

По этому пути можно пойти еще дальше, если использовать так называемую SIM-карту для тестирования.

5.11. АДМИНИСТРАТИВНЫЕ ДАННЫЕ И КАРТЫ ДЛЯ ТЕСТИРОВАНИЯ

Наряду с SIM-картами, предназначенными для обычных или привилегированных клиентов мобильной связи, спецификация GSM предусматривает существование специальных карт, необходимых для технического обслуживания и эксплуатации системы. Такие карты идентифицируются по содержимому их файла AD (7F20:6FAD).

После представления или дезактивации конфиденциального кода CHV1 можно прочитать первый байт файла при помощи следующей последовательности команд:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F AD
A0 B0 00 00 01
```

Полученный результат позволяет отнести карту к одной из представленных ниже стандартных категорий:

- 00: normal operation – обычный режим работы (обычная SIM-карта);
- 80: type approval – подтверждение типа (карта предназначена для тестов на соответствие);
- 01: normal + specific facilities – обычные + специальные функции;
- 81: type approval + specific facilities – подтверждение типа + специальные функции;
- 02: maintenance – техническое обслуживание (off line);
- 04: cell test – тестирование соты.

Карта для тестирования, работающая в некоторых мобильных телефонах фирмы Motorola (иногда продаваемая за 1000 и даже более франков), может быть также реализована, если первый байт ее файла AD получит значение 81h, а самой карте будет присвоен код сети 001-01 (MCC = 001, MNC = 01), при этом идентификационный номер IMSI программируется следующим образом:

```
80 90 01 01 XX XX XX XX XX
```

Учитывая, что номер IMSI записывается в инвертированном виде, в файле 7F20:6F07 можно записать:

```
08 09 10 10 10 32 54 76 98
```

Запись в файле AD, как и в IMSI, может производиться только после представления кода администратора ADM1 (8 байт).

Предположим, что в ASCII этот код имеет вид «ADMINIST». После преобразования в шестнадцатеричный формат он может быть представлен в виде последовательности команд, выполнять которую лучше сразу после сброса карты (подачи на нее напряжения питания):

```
A0 20 00 0B 08 41 44 4D 49 4E 49 53 54
```

Если этот код правильный, то полученный отчет 90 00 будет свидетельствовать об успешном выполнении операции.

Очевидно, что операторы не раскрывают код ADM1 выпускаемых ими карт своим клиентам и тем более код ADM4, позволяющий, в частности, прочитать или изменить код ADM1. Поэтому не следует превращать в карту для тестирования обычную SIM-карту, у которой, например, закончился срок действия.

На имитаторы SIM-карты, построенные на базе микроконтроллера PIC (этот вопрос был рассмотрен в главе 4), естественно, такое ограничение не распространяется.

Другой, еще более соблазнительной возможностью является использование «открытой операционной системы» чип-карты, например, карты «BasicSIM» (см. главу 4), которая предоставляет совершенно свободный доступ к следующим файлам:

```
3F00:2FE2 (ICCID)
7F10:6F3A (ADN, Abbreviated Dialling Numbers)
7F10:6F3B (FDN, Fixed Dialling Numbers)
7F10:6F3C (SMS, Short Messages)
7F10:6F3D (CCP, Capability Configuration Parameters)
7F10:6F40 (MSISDN, Own Numbers)
7F10:6F42 (SMSP, Short Messages Service Parameters)
7F10:6F43 (SMSS, SMS Status)
7F10:6F44 (LND, Last Number Dialed)
7F20/7F21:6F05 (LP, Language Preference)
7F20/7F21:6F07 (IMSI, International Mobile Subscriber Indentity)
7F20/7F21:6F20 (Kc, Ciphering Key)
7F20/7F21:6F30 (PLMN, Preferred PLMNs)
7F20/7F21:6F31 (HPLMN search period)
7F20/7F21:6F38 (SST, SIM Service Table)
7F20/7F21:6F3E (GID1, Group Identifier level 1)
7F20/7F21:6F3F (GID2, Group Identifier level 2)
7F20/7F21:6F74 (BCCH, Broadcast Control Channels)
7F20/7F21:6F78 (ACC, Access Control Class)
7F20/7F21:6F7B (FPLMN, Forbidden PLMNs)
7F20/7F21:6F7E (LOCI, Location Information)
7F20/7F21:6FAD (AD, Administrative Data)
7F20/7F21:6FAE (Phase)
```

Запись в IMSI такой карты может быть следующей:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F 07
A0 D6 00 00 09 08 09 10 10 10 32 54 76 98
```

Запись в AD может иметь, например, такой вид:

```
A0 A4 00 00 02 7F 20
A0 A4 00 00 02 6F AD
A0 D6 00 00 01 81 или A0 D6 00 00 03 81 FF FF
```

В любом случае надо получить отчет 90 00, чтобы убедиться в правильном выполнении операции.

Если вставить карту в совместимый с ней мобильный телефон марки Motorola и в течение приблизительно трех секунд нажимать на клавишу #, то можно войти в режим тестирования. После этого появляется

возможность вести диалог с операционной системой мобильного телефона при помощи следующих команд, выбранных среди наиболее безобидных:

- 19# – воспроизводит номер версии программного обеспечения;
- 58# – воспроизводит код защиты;
- 59# – воспроизводит код «запирания» телефона (но не «отпирания»);
- 01# – позволяет выйти из режима тестирования.

Для проведения дальнейших исследований потребуется серьезная документация (которую можно отыскать в Internet). В противном случае дилетантское использование некоторых команд может привести к выводу из строя мобильного телефона или даже нарушению работы сетей.

На самом деле, если мобильный телефон, снабженный такой картой, не пытается самопроизвольно зарегистрироваться в какой-либо сети, применяемые команды, наоборот, могут инициировать этот процесс, со всеми вытекающими отсюда последствиями.

5.12. ПРОМЫШЛЕННЫЕ СЧИТЫВАЮЩИЕ УСТРОЙСТВА И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Если у вас нет желания или времени заниматься изготовлением собственного «инструментального комплекта» GSM, то все необходимое без проблем можно купить в готовом виде.

Действительно, все большее число производителей устройств для считывания чип-карт общего пользования начинают понимать, какой огромный потенциальный рынок сбыта представляют собой владельцы мобильных телефонов, имеющие ПК, и приступают к разработке программного обеспечения именно для этой категории пользователей.

Бессмысленно отрицать, что подобные прикладные программы, как правило, созданные для Windows, значительно удобнее в работе, чем непосредственный набор команд ISO. Их мощные возможности по работе с базами данных позволяют заняться областью, которая до этого момента тщательно оберегалась. Речь идет об управлении линейными и циклическими файлами, которые слишком объемны, чтобы ими можно было манипулировать «напрямую».

Поэтому, когда возникает необходимость обновлять на ПК хранящиеся в памяти SIM-карты списки телефонных номеров и короткие сообщения, лучше прибегать к помощи специализированного программного обеспечения и соответствующего считывающего устройства (см. рис. 5.5).

Рис. 5.5. Некоторые из предлагаемых промышленных комплектов программного обеспечения

Вместе с тем промышленные устройства для считывания чип-карт позволяют также исследовать SIM-карты при помощи команд ISO, причем со значительно большим удобством, чем при непосредственном использовании DOS.

Для работы со считывающими устройствами, способными функционировать в режиме PC/SC (как, например, CyberMouse), можно использовать утилиту PCSC.EXE (или SCARD.EXE), любезно предоставленную ее производителем. Эта программа установится автоматически после инсталляции драйвера, находящегося на компакт-диске в каталоге ACS.

Будьте внимательны, эта программа ожидает команды, формат которой (APDU) слегка отличается от описанного выше (шесть байт заголовка вместо пяти).

Единственный байт длины (пятый) при этом заменяется двумя байтами: Lc (количество данных, посылаемых SIM-карте) и Le (количество данных, ожидаемых SIM-картой). Если байт длины не используется, достаточно просто записать 00h.

Таким образом, команда A0 A4 00 00 02 7F 20 будет иметь вид A0 A4 00 00 02 00 7F 20, при этом два байта «входных данных» должны быть введены в предназначенное для этого поле (DataIn).

Напротив, команда A0 B0 00 00 04 имеет вид A0 B0 00 00 00 04 (разумеется, поле входных данных должно остаться пустым). В обоих случаях для посылки команды SIM-карте необходимо щелкнуть по кнопке **Exchange APDU**; результат выполнения команды будет выведен в предназначенной для этого области экрана.

После запуска программы PCSC.EXE необходимо выбрать используемое считывающее устройство PC/SC, даже если оно единственное. Для этого нужно щелкнуть по кнопке в области **Card Reader**, а затем выбрать считывающее устройство в появившемся списке.

Наконец, после установки SIM-карты в считывающее устройство нужно в обязательном порядке послать карте команду на сброс (reset), щелкнув по соответствующей кнопке.

На прилагаемом к книге компакт-диске представлены программы, специально разработанные для считывающих устройств ChipDrive фирмы Towitoko. Программа GSMISO.EXE, полностью написанная мною на Delphi 32 бит, включает в себя все функции, которых часто не хватало в инструментарии более общего характера. С ее помощью вы гораздо быстрее усвоите синтаксис команд ISO для SIM-карт. Наличие широкого диапазона подсказок основных полей команд позволяет выиграть время, по сравнению, например, с программами, представленными в главе 4.

По степени усовершенствования промышленное программное обеспечение можно разделить на три уровня:

- средний (light) – создает значительно более удобный доступ к главным функциям, содержащимся в меню мобильного телефона (как минимум, к управлению директориями и короткими сообщениями);
- профессиональный (pro) – позволяет применить бóльшую часть возможностей, которые открываются после представления PIN-кода владельца;
- экспертный (expert) – разрешает, в частности, операции, требующие представления кодов администратора.

В продаже можно найти немало готовых разработок, где, как правило, сочетаются программное обеспечение для Windows и очень специфическое устройство для считывания чип-карт. Можно приобрести все, начиная от миниатюрного считывающего устройства, подключающегося к последовательному порту, и до адаптера, позволяющего подключить SIM-карту к порту USB или даже установить ее в устройство для считывания дискет 3,5".

Наиболее поразительным является тот факт, что стоимость достаточно схожих программных продуктов может различаться в десятки раз. При этом самые дорогие программы не обязательно являются лучшими.

Я выделил из общей массы четыре пакета программ: два немецких, один английский и один... китайский. Кроме того, в этой главе рассматривается еще один пакет программ (английский), который называется «PhoneFile». В средней версии эта программа представлена на компакт-диске в каталоге PCSC.

Не является ли настороженность французских операторов причиной, по которой Франция, являющаяся лидером в области чип-карт, так сдержанно относится к этому сектору рынка? В то же время некоторые немецкие операторы потратили годы, поддерживая практику поставки готовых считывающих устройств своим клиентам.

Программа SIMSurf представляет собой разработку фирмы Towitoko (http://www.towitoko.de), являющейся производителем считывающих устройств ChipDrive, а программа EDSIM 2000 была разработана британским дистрибьютором (http://www.crown.hill.co.uk).

SIMSurf существует в средней и профессиональной версиях. На компакт-диске представлена средняя версия.

EDSIM 2000 бесспорно подпадает под категорию экспертных. Это достойный преемник программы EDSIM1, в средней версии предложенный фирмой Crownhill с комплектом ChipDrive Micro CDSK02. Отметим, что комплект CDSK02, информацию о котором который можно найти на сайте фирмы по адресу http://www.crownhill. co.uk, объединяет по вполне приемлемой цене ChipDrive Micro и набор команд, ориентированных на SIM.

Диапазон возможностей программы EDSIM 2000 впечатляет, но для ее использования потребуются ADM-коды карт, с которыми должна вестись работа.

Как EDSIM 2000, так и SIMSurf зависят от драйвера CardServer, автоматически устанавливаемого одновременно с программой. Лучше всего приобрести (через Internet) его самую последнюю версию.

Версию 2.14.11 данного драйвера вы найдете в каталоге Chipdrive на компакт-диске (для установки нужно просто выполнить программу setuptwk.exe). Данный драйвер потребуется и для работы предлагаемой автором программы GSMISO.EXE со считывающим устройством ChipDrive.

Несмотря на вполне доступную цену пакет программ фирмы «ELV Elektronik» (http://www.elv.de) является, без сомнения, наиболее

мощным (быть может, с точки зрения некоторых, даже слишком мощным) среди имеющихся на рынке. К сожалению, выпускаемое этой фирмой считывающее устройство «ELV Chipcard Reader EasyCheck» (GSCR Velleman) не совместимо с режимом PC/SC. С другой стороны, благодаря этому оно не требует установки драйвера.

Эта программа предоставляет пользователю гораздо больше возможностей, чем ведение персональной телефонной книги. Фактически, пользователь может выполнять практически любые действия, вплоть до аннулирования («запирания») или восстановления («отпирания») файлов на SIM-карте. Справочная система программы (на французском языке) является настоящим хранилищем информации, касающейся возможностей SIM-карт. Кроме того, имеется возможность регулярного обновления программы через Internet (http://www.teledata-update.de). Это позволяет оперативно вносить в нее такие постоянно изменяющиеся данные, как список сетей роуминг-партнеров определенных операторов (что весьма может пригодиться перед поездкой за границу).

В каталоге ELV на компакт-диске вы найдете полнофункциональную версию этой программы (при отсутствии считывающего устройства EasyCheck программа работает в демонстрационном режиме).

Наконец, рассмотрим SIMmate 2000, продукт гонконгской фирмы Advanced Card Systems (http://www.acs.com.hk). Этот комплект, предназначенный для распространения по всему миру, был впервые представлен на выставке «CARTES 2000». Он включает в себя считывающее устройство ACR30 (подключается к компьютеру через последовательный порт или порт USB, поддерживает режим PC/SC) и соответствующее программное обеспечение в средней версии. Возможности программы ограничиваются выполнением тех же действий, которые осуществляются с помощью клавиатуры мобильного телефона. Соответственно, это программное обеспечение совершенно безопасно: риск «убить» SIM-карту при его использовании не больше, чем при правильной эксплуатации мобильного телефона.

В заключение добавим, что после установки дополнительных драйверов считывающее устройство, входящее в комплект, может использоваться с любым программным обеспечением PC/SC, как представленным в данной книге, так и полученным из других источников.

Управление директориями

Основная функция любой программы для SIM-карты (даже принадлежащей к средней категории) заключается в удобном управлении

директориями с номерами телефонов, записанных на карте. Действительно, что может быть скучнее, чем заполнять или исправлять записи в телефонных книжках с помощью клавиатуры телефона, притом что современная SIM-карта в состоянии зарегистрировать, по крайней мере, 100 или 150 номеров.

Программа EDSIM 2000 может управлять не только обычной телефонной книжкой (ADN), но также и фиксированными номерами (FDN), собственными номерами пользователя (MSISDN) и последними набранными номерами (LDN).

Программой SIMSurf предоставляются и дополнительные возможности, такие как классификация в алфавитном порядке и присвоение международных номеров (например, автоматическая замена префикса 0 на + 33).

Наиболее распространенным операционным режимом является считывание исходного содержимого карты, его сохранение на жестком диске или дискете, обработка при помощи редактора, входящего в программное обеспечение, и затем повторная запись на карту, с «забивкой» или без «забивки» предыдущего содержания.

Помимо этого можно импортировать справочники с основных офисных программ (включая таблицы), а также передавать списки с одной SIM-карты на другую (в случае использования нескольких мобильных телефонов).

Управление короткими сообщениями

Пользователь услуг службы коротких сообщений (SMS) не всегда отдает себе отчет в том, что все получаемые и передаваемые сообщения проходят через память SIM-карты, из-за чего и возникает необходимость время от времени ее «чистить» во избежание перегрузки.

Мобильные телефоны позволяют просматривать (на дисплее) получаемые сообщения и в зависимости от модели с помощью клавиатуры составлять собственные.

Если вставить SIM-карту в считывающее устройство для ПК, то появляется возможность просматривать, сохранять, выводить на печать или без труда составлять свои собственные сообщения, а также получать доступ к некоторым «скрытым» характеристикам сообщений, таким как номер SMSC, через который они проходят. Подобная информация является неисчерпаемым источником сюрпризов. Так, например, сообщение, посланное бесплатно через Internet, элементарно может быть передано через Южную Африку (+27) или Сингапур (+65), сделав небольшой крюк через Швейцарию (+41), и все это менее, чем за десять секунд!

Управление сетями

Большую часть времени пользователь предоставляет телефону возможность самому подключаться к сети, за исключением тех случаев, когда он находится за пределами своей страны.

Как мы уже видели, роуминг, то есть использование мобильного телефона за границей, остается одной из самых впечатляющих возможностей системы GSM.

В этом случае выбор сети становится несколько более «деликатным», поскольку в конкретной стране, как правило, существует несколько конкурирующих операторов, готовых предоставить свои услуги, при условии, что используемый мобильный телефон является двухдиапазонным.

Часто пользователю имеет смысл самому составить список сетей, которым он отдает предпочтение (PLMN) в зависимости от страны или даже просто региона, в который он отправляется. Обычно эта функция отсутствует в «средней» версии, но присутствует в «профессиональной» и, конечно, «экспертной».

Кроме того, интересной представляется возможность доступа к списку «запрещенных сетей» (FPLMN), то есть сетей, к которым мобильный телефон даже и не будет пытаться подключиться, если ему не дать соответствующей команды вручную. В принципе, такой список составляется автоматически, по мере поступления отказов на попытку подключения к сети во время перемещений мобильного.

Наряду с этим ничто не мешает периодически стирать или, наоборот, добавлять коды операторов, в услугах которых более не нуждаются (например, в приграничной зоне, во избежание попадания на сеть соседнего государства, где услуги связи могут стоить достаточно дорого).

Управление секретными кодами

Как правило, конфиденциальный код (PIN или CHV1) должен набираться при каждом включении телефона в целях безопасности на случай кражи или потери. Выше уже говорилось, что контроль за данной функцией осуществляется только SIM-картой. Иногда это может быть дополнено вторым кодом (PIN2 или CHV2) для защиты некоторых специальных функций.

PIN-код может дезактивироваться, изменяться и вновь активироваться по желанию пользователя либо с помощью меню телефона, либо командами ISO, либо с ПК.

В том случае, если код набирается неправильно три раза подряд (даже при выключении телефона или вынимании из него карты между двумя попытками), SIM-карта блокируется. Для того чтобы ее разблокировать, требуется еще один код (super PIN или PUK[1]), который выдается оператором после проверки паспортных данных своего клиента.

Обычно этот код вводится с помощью клавиатуры в соответствии со специфической процедурой, так называемой **04* для PIN1 и **042* для PIN2. Намного удобнее это делать с помощью компьютера, оснащенного программным обеспечением профессионального или экспертного уровня.

Исследование SIM-карты

Выше уже шла речь о том, что при помощи различных команд ISO после предварительного введения конфиденциального PIN-кода владелец SIM-карты может свободно ознакомиться со многими ее параметрами.

При щелчке мышью по опции **Info** (Информация) программы профессионального и экспертного уровня выдают детальный отчет о том, какая информация может быть прочитана. Следует отметить, что программа EDSIM 2000 значительно лучше оснащена, чем SIMSurf, однако ни одна из этих двух программ не в состоянии полностью исследовать наиболее поздние модели SIM-карт (фаза 2+, SIM Toolkit или Proactive SIM).

Для того чтобы продвинуться в изучении дальше, следует обратиться к командам ISO или режиму редактирования, имеющемуся в программах профессионального и экспертного уровня. Эта мощная функция позволяет считывать содержимое в шестнадцатеричном формате, даже ASCII, различных зон SIM-карты, доступ к которым дают имеющиеся в распоряжении коды.

Возможно даже внесение изменений, хотя такая операция является довольно рискованной (и программы выводят напоминающие об этом сообщения).

EDSIM 2000 представляет собой одну из редких программ, позволяющих выбирать файл не только при помощи ограничивающего возможности меню, но также и путем свободного указания адреса, что несколько напоминает использование команд ISO.

---

[1] Personal Unblocking Key – персональный (личный) ключ для разблокирования карты. – *Прим. науч. ред.*

Кроме того, EDSIM 2000 располагает таким сильным инструментарием, как снупер (snooper). Путем проведения систематического просмотра и очистки он определяет, какие файлы (стандартные или нет) находятся на карте, позволяя затем их по желанию проверять.

Похожую возможность предоставляет SimScan, программа общего пользования (см. каталог Internet на компакт-диске). С ее помощью при использовании считывающего устройства для SIM-карт, описанного в главе 4 (в данном случае в обязательном порядке подключенного к порту COM2), можно определить криптографический ключ, если потратить на это несколько часов.

Копии SIM-карт

Ни одна из представленных промышленных программ не может использоваться для непосредственного «клонирования» SIM-карт, иначе говоря, для создания действующих дубликатов исходной карты.

Данные, реализующие абонемент (или услугу на основе предварительной оплаты), располагаются в зонах, защищенных кодами ADM, и ни при каких условиях не должны покидать базы данных оператора мобильной связи.

Поэтому функции копирования служат только для абсолютно легальной передачи данных владельца с одной SIM-карты на другую. Это может оказаться весьма полезным при смене оператора, абонемента или SIM-карты, при приобретении нового мобильного телефона или когда требуется, чтобы все мобильные одной семьи (или предприятия) содержали директории с одними и теми же телефонными номерами.

5.13. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ СЧИТЫВАЮЩИХ УСТРОЙСТВ PC/SC

Нет сомнений, что когда-нибудь практически все выпускаемые микрокомпьютеры, работающие под управлением Windows, будут оснащаться устройством для считывания чип-карт, или, по крайней мере, клавиатурой, имеющей такую возможность.

Вполне возможно, что данные считывающие устройства будут соответствовать спецификации «PC/SC» и, следовательно, будут совместимы с программным обеспечением, поддерживающим этот широко признанный стандарт. А пока можно использовать некоторые промышленно выпускаемые считывающие устройства для работы

в режиме PC/SC (например, модели «ChipDrive» фирмы Towitoko, «CyberMouse» фирмы ZietControl (см. рис. 5.6), ACR20 или ACR30 фирмы ACS и различные модели USB или PCMCIA).

Рис. 5.6. Считывающее устройство PC/SC из комплекта BasicCard

Однако, несмотря на несомненное преимущество промышленного программного обеспечения, мне хотелось разработать пакет программ PC/SC, позволяющий достаточно подробно исследовать любую SIM-карту. При этом использовался «специальный язык чип-карт», являющийся модификацией старого доброго Бейсика (см. мою книгу «Basic pour microconlroleurs et PC»).

Хотя ZCBasic предназначен прежде всего для поддержки знаменитой BasicCard (см. рис. 5.7), о которой говорилось в главе 4, он прекрасно подходит и для написания приложений чуть ли не для каждой асинхронной чип-карты.

Главное преимущество подобного инструментария состоит в том, что он может использоваться свободно и бесплатно. Вы найдете его на компакт-диске, который прилагается к настоящей книге (каталог BASICCARD). Но для того, чтобы устройство для считывания чип-карт работало в режиме PC/SC, необходимо оснастить ПК различными программными «слоями», которые схематично представлены на рис. 5.8.

Рис. 5.7. Внешний вид комплекта BasicCard

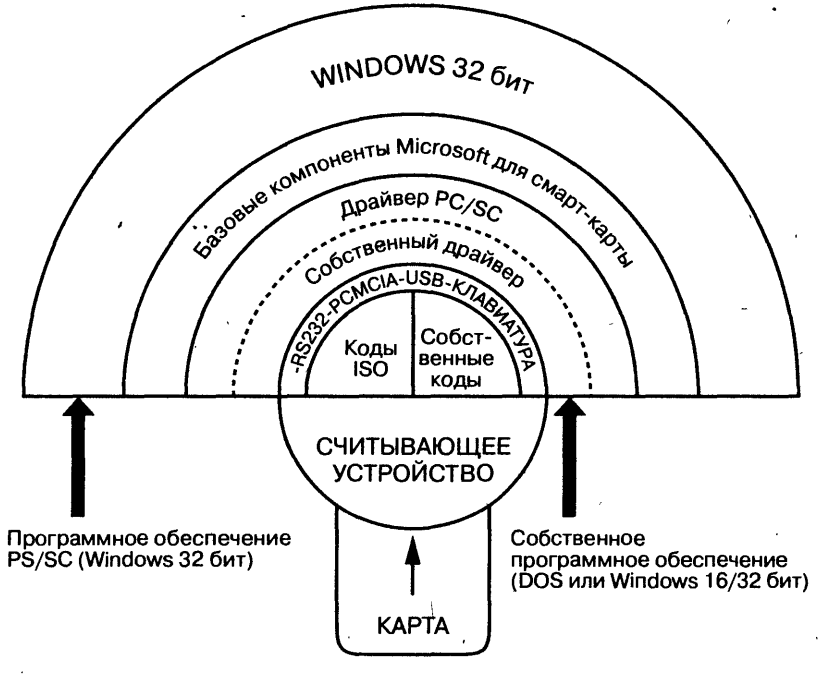


Рис. 5.8. Программная организация совместимости с PC/SC

Прежде всего, это библиотеки «Smart Card Base Components» (базовые компоненты для смарт-карт) фирмы Microsoft (SCBASE.EXE и SMCLIB.EXE), если используется версия Windows (32 бит), изначально не поддерживающая чип-карты (например, Windows 95 или 98).

Затем драйвер PC/SC для применяемого считывающего устройства (не путать с «родным» драйвером считывающего устройства).

В принципе, если все программные элементы установлены правильно, то считывающее устройство будет функционировать в режиме PC/SC, если оно уже было подсоединено к ПК, когда на компьютер подали питание.

Напротив, «родной» режим будет единственно доступным, если считывающее устройство подключают к ПК (например, с помощью ручного переключателя) уже после запуска Windows.

Можно провести диагностику правильности установки одного или нескольких считывающих устройств PC/SC при помощи специализированных утилит, таких как PCSCINF.EXE, любезно предоставленных фирмой ZeitControl (каталог PCSC прилагаемого компакт-диска), или QUICKTEST.EXE (доступной после установки драйвера из каталога ACS).

Прежде чем запустить любую из перечисленных утилит, необходимо вставить какую-либо асинхронную карту.

Все программное обеспечение написано для работы на ПК, оборудованным одним считывающим устройством PC/SC (если установлено несколько устройств, то будет задействовано устройство №1).

Пользователю, очевидно, следует приобрести «Smart Card Base Components» у Microsoft, а необходимые драйверы – у поставщика используемого считывающего устройства (некоторые из них содержатся в поддиректории DRIVERS каталога ACS на компакт-диске).

На тот случай, если у вас возникнут какие-либо проблемы при работе считывающего устройства PC/SC, я скомпилировал свои программы и для «родного» последовательного режима считывающего устройства CyberMouse, поставляемого в комплектах BasicCard (подкаталоги COM_1 и COM_2). Для этого было достаточно заменить в исходном коде строку «ComPort=101» на «ComPort=1» или «ComPort=2» в зависимости от того, к какому порту подключено считывающее устройство: к COM1 или COM2.

Следует отметить, что программы, работающие в консольном режиме Windows, визуально очень напоминают режим командной строки DOS.

Позже вы увидите, как посредством среды программирования Delphi можно добавить к этим программам все преимущества графического интерфейса Windows.

Программа диагностики

DIAGSIM.EXE – это программа, позволяющая знакомиться с характеристиками SIM-карты, вставленной в считывающее устройство, в режиме просмотра (без возможности делать какие-либо изменения).

Данная программа, в сущности, воспроизводит исследование, которое осуществляется мобильным телефоном при включении питания и позволяет ему автоматически адаптироваться к возможностям карты.

Совместимость ELP (Extended Language Preference) и TP (Terminal Profile) касается, в принципе, только карт «Фазы 2+» или «STK» (SIM Toolkit), способных, тем не менее, работать в телефоне фазы 1 или 2. Нормальный ход процесса исследования предполагает, что конфиденциальный код (PIN или CHV1) предварительно был дезактивирован.

Это можно сделать при помощи меню телефона (перед тем как вытащить карту) или при помощи разработанной мной программы SIMPIN.EXE (она предназначена для дезактивирования кода, если он был активирован и наоборот).

Затем можно будет ознакомиться с состоянием кодов CHV1, CHV2, PUK1 и PUK2, а потом с разного рода информацией, как правило, не отображаемой на экранах телефонов, чтение которой разрешено строго после представления кода CHV1.

Полное декодирование таблицы SST (SIM Service Table) может, в частности, дать сведения по еще неиспользованным возможностям карты, а раскодировка классов доступа пояснит различие в приоритетах доступа в сеть между разными тарифными схемами: по абонементу или с предварительной оплатой.

Программа сканирования SIM-карты

Программа SNOOP.EXE является упрощенной версией того, что обычно называют snooper, или «сыщик». Эта программа систематически проверяет наличие основных стандартных файлов в корневой директории и директориях Telecom, GSM и DCS.

Поскольку на компакт-диске представлен ее исходный код (см. подкаталог SOURCES), можно легко перекомпилировать программу при помощи ZCBasic, изменяя по желанию границы установленного поиска.

Это позволяет обнаруживать нестандартные файлы (которые существуют почти всегда), однако значительно увеличивает длительность поиска (несколько десятков минут или более). Во время выполнения

программы SNOOP.EXE результаты поиска отображаются на экране дисплея и записываются в файл SNOOP.LOG. Их подробный анализ после окончания сканирования осуществляет программа DSNOOP.EXE, которая выводит на экран имена стандартных файлов.

Для «прокручивания» всего списка необходимо нажимать на клавишу «пробел» на клавиатуре, так как количество выводимой информации может быть достаточно велико.

Естественно, имена файлов отображаются на английском языке, строго в соответствии со стандартом GSM 11.11, официально публикуемом только на этом языке.

В каталоге PCSC на компакт-диске вы найдете файлы, записанные с настоящих SIM-карт, – PHASE1.LOG и PHASE2.LOG. Их изучение позволит понять эволюцию, произошедшую между фазой 1 и фазой 2 спецификации GSM.

При желании можно проанализировать их при помощи программы DSNOOP.EXE, но для этого сначала их следует по очереди переименовать в SNOOP.LOG.

Проверка криптографии

GSM.EXE представляет собой небольшую программу, задача которой – требовать от SIM-карты выполнения алгоритма аутентификации (A3/A8) на основе неизменного блока из 16 байт.

Так, мы произвольно запрограммировали последовательность ASCII «AUTHENTIFICATION» вместо случайной величины, обычно предоставляемой сетью. Известно, что полученный результат состоит из подписи SRES (4 байта) и ключа шифрования K_c (8 байт). Разумеется, эти значения должны быть различными у разных SIM-карт, поскольку каждая из них имеет свой собственный секретный ключ K_i. И, напротив, они не должны отличаться при повторных обращениях к одной и той же карте.

Интересно проанализировать результат K_c, чтобы установить, насколько часто его значение заканчивается десятью нулевыми битами (байт 00h предшествует байту, два последних бита которого равны нулю).

Выполнение этого условия означает снижение «криптостойкости» (или «энтропии») алгоритма A5 до 54 бит вместо 64-х, предусмотренных стандартом, другими словами – уменьшение в 1024 раза! А обычно считается, что шифрование в 56 бит (в четыре раза сильнее) уже никуда не годится.

Такое преднамеренное ослабление безопасности обмена данными практически не представляет какого-либо технического или экономического интереса для операторов, возможно, это является требованием властей, наделенных полномочиями прослушивания телефонов.

Было бы интересно подвергнуть этому тесту SIM-карты, выпущенные операторами различных стран, подключение к данному алгоритму «по умолчанию» вовсе не обязательно, это всего-навсего самое легкое решение.

«Навигатор» для SIM-карты

Несмотря на некоторую примитивность, эта небольшая программа часто оказывается более эффективной, чем лучшие из промышленных программ, когда необходимо «вслепую» исследовать SIM-карту.

Программа NAVSIM.EXE, работающая в консольном режиме Windows, сочетает строгость DOS-приложений с поддержкой PC/SC, доступной только в Windows 32 бит.

Одна единственная команда (SELECT) позволяет свободно перемещаться по структуре директорий, поддиректорий и файлов любой SIM-карты, если известны их шестнадцатеричные адреса (в результате предварительного выполнения программы SNOOP.EXE).

При запуске программы по умолчанию выбирается корневая директория (3F00h), что позволяет, например, сразу получить доступ к файлу ICCID, просто набрав 2FE2. После этого выводятся подробные характеристики рассматриваемого файла, начиная от его размера до списка кодов, необходимых для осуществления различных текущих операций (чтение, запись, объявление недействительным, восстановление и т.д.).

Если считывание (read) возможно (разрешено изначально или в результате предварительного дезактивирования PIN-кода), оно осуществляется автоматически за один раз.

Если запись (update) также разрешена, то новые значения байтов можно ввести (с учетом всех пробелов) непосредственно под отображающимися на экране только что считанными значениями. Однако запись на карту в действительности произойдет только тогда, когда эти изменения будут подтверждены возвратом к началу строки.

Значения первых байтов должны быть введены даже в том случае, если они не изменяются. Вместе с тем, набор можно прекратить, как только будет введен последний изменяемый байт. Если ни один байт не изменяется, достаточно просто вернуться к началу строки (нажав на клавишу **Enter**), ничего не набирая.

Если есть место, то повторное контрольное считывание выполняется следом, автоматически, а результат выводится строкой ниже. В этом случае можно выполнить новую модификацию или же вернуться к началу строки, чтобы выбрать новый файл или директорию. Его шестнадцатеричный адрес, естественно, может быть набран только после появления приглашения «SELECT».

На этом этапе можно выйти из программы: достаточно просто вернуться к началу строки, ничего не печатая после «SELECT».

Несколько более сложным является вариант, когда выбранный файл состоит из записей (records) достаточно большого размера. В этом случае необходимо дополнительно нажать на **Enter** для приостановки режима считывания, чтобы успеть прочитать уже выведенные на экран данные.

По соображениям безопасности возможность записи в файлы этой категории не предусмотрена. Модификация директорий телефонных номеров и SMS-сообщений может осуществляться только в среде базы данных. Это предполагает использование промышленного программного обеспечения, которое может быть и совместимым с PC/SC, и бесплатным (например, программа PhoneFile, представленная в средней версии на компакт-диске. Для работы с ней требуется получить личный пароль по адресу http://www.pipistrel.com/phonefile).

Заметим, что PhoneFile поддерживает множество различных устройств для считывания чип-карт, в том числе и считывающие устройства ChipDrive, которые при этом должны использоваться исключительно в своем «родном» режиме и, следовательно, подключаться только после успешной загрузки Windows. Напротив, считывающее устройство CyberMouse из комплекта BasicCard должно применяться в режиме PC/SC и, значит, снабжаться собственным драйвером.

С целью безопасности в программе NAVSIM.EXE не предусматриваются ни функции представления кодов, ни функции блокирования/восстановления файлов.

Известно, что код CHV1 может быть предварительно дезактивирован при помощи программы SIMPIN.EXE, тогда как коды ADM (коды администратора) не предназначены для того, чтобы их знали обладатели SIM-карт.

Операции блокирования и восстановления файлов, в свою очередь, наиболее часто осуществляются мобильным телефоном и/или сетью в «прозрачном» режиме (например, чтобы заблокировать доступ к директории ADN, если ограничиваются вызовом фиксированных номеров FDN), тогда как некорректное блокирование будет с большой вероятностью необратимым.

Разумеется, эти ограничения не распространяются на нашу инструментальную карту BasicSIM (см. главу 4), которая предлагает безусловный доступ ко всем своим файлам.

Интеграция в графический интерфейс Windows

Приложения, разработанные под ZCBasic, вызывают некоторую ностальгию по GWBasic и режиму «командной строки» DOS, но следует признать, что этот строгий интерфейс отталкивает пользователей, привыкших к графическому интерфейсу Windows.

Поэтому я и решил написать на ZCBasic функции, наиболее тесно взаимодействующие с SIM-картой, и вызывать их из разработанного под Delphi приложения. Вызовы осуществляются с использованием (в развернутом или свернутом окне) функции Windows `CreateProcess` и довольно упрощенной системы передачи данных при помощи файла на диске.

На современном и, следовательно, достаточно мощном компьютере потеря времени из-за использования такого операционного режима вполне приемлема для этой модели, рассчитанной на «двойную отладку» в комплекте BasicCard.

Разработанное мной приложение SIMPCSC.EXE предназначено для считывания двух основных идентификационных номеров любой SIM-карты: ICCID (номер карты, не составляющий никакого секрета) и IMSI (международный идентификационный номер абонента, считывание которого защищено PIN-кодом).

Эта работа предназначается для новой программы ZCBasic, SIM.EXE, тогда как программа SIMPIN.EXE будет просто задействована для дезактивирования PIN-кода, если он активирован, при условии, что он вновь будет активирован после прочтения IMSI.

Полный проект, следовательно, состоит из двух отдельных программ ZCBasic, реализующих базовые функции, и очень простой программы Delphi 3, обеспечивающей работу этих программ в режиме окна, снабженного кнопками, в стиле Windows.

Для запуска каждой из двух программ предназначены различные кнопки. Программа SIMPIN.EXE запускается в окне MS DOS, а SIM.EXE – в окне, которое отображается только на панели задач (что позволяет открыть его в случае каких-либо проблем).

Результаты, которые программа SIM.EXE обычно выводит на экран, остаются скрытыми, но при этом они записываются в файл SIM.SIM. Именно оттуда их извлекает приложение Delphi, чтобы затем с некоторой «режиссурой» показать на экране.

Разумеется, этот метод может использоваться и с другими программами ZCBasic.

5.14. ПРОГРАММЫ, РАЗМЕЩЕННЫЕ НА КОМПАКТ-ДИСКЕ, И ПРИЛОЖЕНИЯ

Помимо программ, написанных мною и составляющих, в частности, программное обеспечение для предложенных схем, в приложениях к данной книге вы найдете программы и документы, предоставленные отдельными производителями, а также находящиеся в свободном доступе в сети Internet.

Демонстрационные версии промышленных продуктов могут работать и без считывающего устройства чип-карт, поскольку они просто имитируют присутствие настоящей SIM-карты. Они позволяют оценить и сравнить различные типы инструментария, предлагаемого на рынке, а также служат источником ценной информации, которую, в частности, можно почерпнуть из их системы подсказок.

Найденные в Internet программы были размещены их авторами в свободном доступе и представлены на диске с единственной целью: оказать услугу тем из читателей, которые сами по тем или иным причинам не могут провести аналогичный поиск.

Рекомендуется всегда использовать самые последние версии программ по мере их появления, а также обращать внимание на условия их использования в независимости от того, на каком языке и в какой форме они представлены.

Однако нужно напомнить, что я не несу ответственность за прямые или косвенные последствия применения или простого обладания этими программами, права интеллектуальной собственности на которые принадлежат их авторам.

Учитывая все вышесказанное, давайте рассмотрим, что содержится в каталогах, расположенных на прилагаемом к книге компакт-диске, а также представлено в приложениях.

Каталог ACS

Этот каталог содержит полную документацию в формате PDF на считывающие устройства ACR 20 и ACR 30 фирмы Advanced Card Systems (ACS).

Модель ACR 20 S (для последовательного порта) совместима со считывающим устройством CyberMouse, поставляемым в комплекте BasicCard, которое может использовать тот же драйвер PC/SC. В подкаталоге DRIVERS содержится все необходимое для установки

драйверов практически на любой ПК, имеющий операционную систему Windows 32 бит.

После выполнения файл будет распакован в рабочий каталог. На этом этапе следует внимательно прочитать руководство, представленное в виде PDF-файла, а затем начать установку, дважды щелкнув по значку исполняемого файла SETUP.EXE.

Внимание! Все считывающие устройства ACR или CyberMouse при установке должны быть предварительно выключены, рекомендуется временно деинсталлировать драйверы считывающих устройств другой марки (например, ChipDrive), если они были уже установлены.

Следует отметить, что сосуществование нескольких считывающих устройств PC/SC различных марок может являться неисчерпаемым источником разного рода «сюрпризов».

Каталог BASIC

Файлы INVISO.BAS и DIRISO.BAS представляют собой исходный код программ INVISO.EXE и DIRISO.EXE, которые находятся в каталоге LECTSIM.

Напрямую использоваться со считывающим устройством, представленным в главе 4, могут только программы INVISO.EXE и DIRISO.EXE. За любой вынужденной модификацией исходного кода должна последовать соответствующая перекомпиляция.

Программа IMEI.BAS может реализовываться как на GWBASIC, так и на QBASIC, а если у вас нет таких интерпретаторов, воспользуйтесь исполняемой версией (IMEI.EXE).

В среде Windows это приложение MS DOS выполняется в полноэкранном режиме.

Каталог BASICCARD

В этом каталоге содержатся полные версии комплекта разработки BasicCard немецкой фирмы ZeitControl.

Для установки на ПК предлагается профессиональная версия (подкаталог INSTBC4), однако вы можете следить за появлением новых версий программы на сайте http://www.basiccard.com.

Напомним, что речь идет о программной части комплекта, включающего также устройство для считывания чип-карт (CyberMouse) и уникальные карты с открытой операционной системой, полностью программируемые на Бейсике.

Используемый язык, названный ZCBasic, является вариантом (специально для чип-карт) Бейсик-компилятора, генерирующего

исполняемые файлы, которые совместимы с консольным режимом Windows 32 бит и считывающими устройствами PC/SC.

Версия 2 (подкаталог INSTBC2) позволяет также компилировать исполняемые файлы, работающие в обычной системе MS DOS (без подключения Windows), но при этом пропадает совместимость с PC/SC.

Впрочем, нет необходимости устанавливать комплект только для того, чтобы работало представленное в этой книге программное обеспечение PC/SC (кроме случая, когда понадобится перекомпилировать ПО после модификации исходного кода).

Файл BASICCRD.PDF является электронной версией руководства, поставляемого вместе с промышленным комплектом, и содержит все сведения, необходимые для работы.

Каталог BASICSIM

Находящееся в этом каталоге программное обеспечение предназначено для преобразования BasicCard в имитатор SIM-карты, даже если комплект разработки не установлен.

Несколько подкаталогов соответствуют различным версиям BasicCard и содержат файлы с расширением .BAT, позволяющие осуществлять обмен данными с картой через различные модели считывающих устройств (CyberMouse в «родном» режиме или же любое считывающее устройство PC/SC).

Файл IMG, предназначенный для ZC 4.1, соответствует самой последней на момент разработки этого проекта версии «ZC 4.1 RSA 2001.09.28».

Если при появлении новых версий BasicCard возникнет необходимость обновить этот файл, я приложу все усилия, чтобы распространить его через один из сайтов Internet, упоминавшихся в настоящем издании.

Приложение Windows (SIMSPY.EXE) предназначено для считывания с карты записи последовательности команд, направленных ей во время последних сеансов.

Отметим, что файл R.EXE должен присутствовать в той же рабочей директории.

Для сравнения представлены некоторые примеры перехваченных таким образом диалогов. Файл SIMSURF.LOG был записан при помощи BASICSIM «ZC 3.3», управляемого программным обеспечением SIMSurf Profi (см. главу 5), а SIMMATE.LOG – после применения программного обеспечения SIMmate 2000 (http://www.simmate2000.com).

Файлы PH2.LOG и STK.LOG были собраны после установки BasicSIM «ZC 4.1» в два телефона GSM, совместимые с «Фазой 2» и «Фазой 2+».

BSUTIL.EXE, со своей стороны, позволяет легко перейти ко всем операциям инициализации и конфигурирования BasicSIM при помощи любого считывающего устройства PC/SC.

Каталог CHIPDRIVE

Содержимое данного каталога имеет отношение только к устройствам для считывания чип-карт Chipdrive фирмы Towitoko (http://www.towitoko.de).

В нескольких PDF-файлах (которые можно прочитать при помощи программы Acrobat Reader) приводится детальное описание этого семейства считывающих устройств, производимых в Германии и нашедших признание и применение во всем мире.

Файл SETUPTWK.EXE позволяет отдельно установить на ПК версию 2.14.11 драйвера CardServer, совместимого с PC/SC.

Программа GSMISO.EXE может использоваться только после установки этого драйвера и считывающего устройства семейства Chipdrive (рекомендуется модель Micro или Extern).

Отметим, что комплект CDSK02, который можно найти по адресу http://www.crownhill.co.uk, объединяет по вполне приемлемой цене ChipDrive Micro и набор команд, ориентированных на SIM.

Подкаталоги DISK1 и DISK2 содержат файлы, относящиеся к демонстрационной версии SIMSurf (для того, чтобы произвести установку, надо просто выполнить SETUP.EXE).

Каталог CYBMOUSE

Этот каталог содержит полную коллекцию драйверов, необходимых для работы считывающего устройства CyberMouse в режиме PC/SC. Драйверы поставляются в комплекте разработки BasicCard; их также можно получить, обратившись по адресу http:// www.hitechtools.com.

В зависимости от используемой операционной системы следует обращаться к соответствующему подкаталогу, обязательно прочитав при этом указания, которые там содержатся.

Но в некоторых случаях лучше установить сначала полную версию драйвера, которая находится в каталоге ACS, так как при этом открывается доступ к интересным утилитам.

Следует отметить, что если программное обеспечение PC/SC, представленное в данной книге, требует предварительной установки одного из данных драйверов, то комплект разработки BasicCard может функционировать и без этого (тогда используется последовательный режим, «родной» для CyberMouse).

Файл CYBERM.PDF содержит электронную версию справочного руководства, в котором вы найдете все необходимые сведения для работы с этим считывающим устройством.

Каталог ELV

Здесь находится полная французская версия программного обеспечения для управления SIM-картами. При отсутствии специального считывающего устройства «ELV Chipcard Reader EasyChech» ПО работает в демонстрационном режиме. В этом же каталоге содержатся справочное руководство в виде PDF-файла и координаты поставщика программного продукта (файл CONTACT.TXT).

Каталог ESPION

Здесь вы найдете программное обеспечение, предназначенное для схемы «шпиона за SIM-картами» (см. главу 4).

SIMINV.EXE и SIMDIR.EXE являются исполняемыми файлами MS DOS, для которых также имеются исходные коды на Бейсике. Не следует пытаться выполнить их при помощи такого интерпретатора, как GWBasic или QBasic, но в случае внесения в них каких-либо изменений их необходимо перекомпилировать.

Каталог INTERNET

В этом каталоге содержатся файлы ZIP, которые разархивируются при помощи Winzip (в Windows) или PKUnzip (в MS DOS). Они воспроизводятся в том виде, в котором были размещены в Internet их авторами для свободного доступа.

Каталог LECTSIM

Этот каталог содержит исполняемые в MS DOS файлы двух программ, совместимых с устройством для считывания SIM-карт, описанным в главе 4. Перед их выполнением рекомендуется выйти из Windows или даже произвести эту операцию на ПК, работающем только в MS DOS (можно порекомендовать 386 SX 25).

Каталог PCB

В этом каталоге содержатся файлы с расширением .PCB, в которых приводится топология печатных плат устройств, рассмотренных в книге. Файлы созданы при помощи пакета программ Boardmaker.

Сокращенную версию данной программы вы найдете в подкаталоге BMAKER1. С ее помощью можно распечатывать эти рисунки в любом масштабе и даже редактировать их перед выводом на печать. Правда, в отличие от полной сокращенная версия не позволяет сохранять изменения на диске.

Данный пакет программ для MS DOS детально рассмотрен в моих книгах «Logiciels PC pour l'électronique» и «Circuits Imprimés, conceptions et réalisation».

Каталог PCSC

В этом каталоге собраны исполняемые файлы всех приложений, предназначенных для работы со считывающим устройством PC/SC.

Он содержит как разработанные мной программы, написанные на ZCBasic, так и программное обеспечение, предложенное нашими партнерами. Исходный код авторских программ содержится в отдельном подкаталоге (SOURCES).

Чтобы все эти программы нормально работали, устройство для считывания чип-карт, соответствующее стандарту PC/SC, должно быть правильно установлено. В случае сомнений можно воспользоваться программой PCSCINF.EXE, которая позволяет осуществить диагностику одного или нескольких установленных считывающих устройств PC/SC.

За неимением считывающего устройства PC/SC, изначально входящего в состав компьютера или клавиатуры, вполне можно использовать CyberMouse (ZeitControl), ACR20 или ACR30 (ACS) либо ChipDrive (Towitoko), а также большинство считывающих устройств Gemplus.

Наконец, при отсутствии какого-либо считывающего устройства PC/SC можно работать с версиями, предназначенными для «родного» последовательного режима считывающего устройства CyberMouse или ACR20S, содержащимися в подкаталогах COM_1 и COM_2 (в зависимости от используемого последовательного порта).

Каталог SONS

В данном каталоге представлены файлы с расширением .WAV, предназначенные для прослушивания (для этого необходимо на ПК иметь звуковую карту). Четыре из них позволяют сопоставить качество звука, предлагаемого полноскоростными мобильными телефонами (GSM) и обычными проводными телефонами (CCITT). Вы можете сравнить сообщение, передаваемое известным оператором (которое состоит только из слов), и сообщение (состоящее из слов и музыки), заимствованное у его прямого конкурента.

Файл ERREUR.WAV воспроизводит последовательность тональностей, используемых для предупреждения о нестандартных ситуациях. Файл PERTURBE.WAV представляет собой краткую запись помех от мобильного телефона, работающего в непосредственной близости от недостаточно защищенного аудиооборудования.

Словарь GSM

Международный сленг специалистов в области GSM включает более 500 сокращений на английском языке.

На страницах книги были расшифрованы наиболее распространенные из них, хотя речь, конечно, идет о ничтожно малой части того, что можно встретить даже в самом кратком справочном издании.

Если вы захотите продолжить исследование системы GSM, то в Internet сможете найти всю необходимую информацию (особенно на английском языке), начиная со стандартов института ETSI и заканчивая файлами, считающимися конфиденциальными, но которые доступны любому желающему. Ознакомление с этими файлами невозможно себе представить без специализированного словаря, версия которого приведена в разделе 6.1.

Данные по международному роумингу

В нескольких таблицах, приведенных в разделе 6.2, представлена самая последняя информация по сетям операторов мобильной связи GSM со всего мира. Эти данные предоставлены компанией Swisscom, которой принадлежит заслуга подписания наибольшего числа договоров по роумингу. На компакт-диске в каталоге ROAMING имеется

руководство по международной карте с предварительной оплатой GSM CARD easyRoam, которая часто использовалась в качестве примера на страницах книги (карту можно приобрести через Internet на сайте http://www.easy-roam.com). Здесь вы также найдете инструкцию по пользованию голосовым почтовым ящиком ComBox. Некоторые из этих документов могут быть обновлены при помощи бесплатной системы «факс по запросу» (международный бесплатный номер: 00 800 55 65 65 65).

Требования к аппаратному и программному обеспечению

В разделе 6.3 приведены минимальные требования к аппаратному и программному обеспечению компьютера для работы с этой книгой.

6 ПРИЛОЖЕНИЯ

6.1. ГЛОССАРИЙ

A

A3 – Алгоритм аутентификации A3.

A38 – Единый алгоритм выполнения функций A3 и A8.

A5/1 – Алгоритм шифрования A5/1.

A5/2 – Алгоритм шифрования A5/2.

A5/X – Алгоритм шифрования A5/0–7.

A8 – Алгоритм A8 формирования (генерирования) ключа для шифрования.

AB – *Access Burst.* Пакетный сигнал доступа (к сети).

AC – *(1) Access Class (C0 to C15).* Класс доступа (C0–C15).

AC – *(2) Application Context.* Контекст приложения.

ACC – *(1) Automatic Congestion Control.* Автоматическое управление перегрузкой (в сети).

ACC – *(2) Access Control Class.* Класс управления доступом.

ACCH – *Associated Control CHannel.* Совмещенный канал управления.

ACK – *ACKnowledgement.* Подтверждение (приема сообщения).

ACM – *(1) Accumulated Call Meter.* Счетчик накопленных вызовов.

ACM – *(2) Address Complete Message.* Адресация завершенного сообщения.

ACU – *Antenna Combining Unit.* Блок соединения с антенной.

AD – *Administrative Data.* Административные данные.

ADC – *(1) ADministration Centre.* Административный центр (центр управления).

ADC – *(2) Analogue to Digital Converter.* Аналого-цифровой преобразователь (АЦП).

ADN – *Abbreviated Dialling Number.* Ускоренный набор номера.

ADPCM – *Adaptive Differential Pulse Code Modulation.* Адаптивная дифференциальная импульсно-кодовая модуляция.

AE – *Application Entity.* Объект (сущность) приложения.

AEC – *Acoustic Echo Control.* Управление акустическими эхо-сигналами.

AEF – *Additional Elementary Functions.* Дополнительные (добавочные) элементарные функции.

AGCH – *Access Grant CHannel.* Разрешение (предоставление) доступа к каналу.

Ai – *Action indicator.* Индикатор действия (операции).

AoC – *Advice of Charge.* Извещение (предоставление информации) о стоимости разговоров.

AoCC – *Advice of Charge Charging supplementary service.* Дополнительная услуга извещения о пополнении счета.

AoCI – *Advice of Charge Information supplementary service.* Дополнительная услуга предоставления информации о состоянии счета.

ASE – *Application Service Element.* Элемент сервиса приложения.

ASN.1 – *Abstract Syntax Notation One.* Абстрактная синтаксическая нотация версии 1, язык ASN.1 (используется в рамках протокола взаимодействия открытых систем).

ARFCN – *Absolute Radio Frequency Channel Number.* Абсолютное число каналов ВЧ.

ARQ – *Automatic ReQuest for retransmission.* Автоматический запрос на повторную передачу.

ATT – *(flag) ATTach.* Флаг присоединения, прикрепления.

AU – *Access Unit.* Устройство (блок) доступа.

AuC – *Authentication Centre.* Центр аутентификации.

AUT(H) – *AUThentication.* Аутентификация, проверка подлинности.

B

BA – *BCCH Allocation.* Назначение (распределение) BCCH.

BAIC – *Barring of All Incoming Calls supplementary service.* Дополнительная услуга запрета всех входящих звонков.

BAOC – *Barring of All Outgoing Calls supplementary service.* Дополнительная услуга запрета всех исходящих звонков.

BCC – *Base transceiver station (BTS) Colour Code.* Цветовой код базовой приемо-передающей станции.

BCCH – *Broadcast Control CHannel.* Канал управления вещанием (передачей).

BCD – *Binary Coded Decimal.* Двоично-десятичное число (код); представление чисел, при котором каждая десятичная цифра кодируется двоичным эквивалентом длиной четыре бита.

BCF – *Base station Control Function.* Управление работой базовой станции.

BCIE – *Bearer Capability Information Element.* Информационная составляющая характеристики передаваемого сообщения (данных).

BER – *Bit Error Rate.* Частота (вероятность) появления ошибочных битов.

BFI – *Bad Frame Indication.* Индикация ошибочного (неправильного) кадра.

BI – *all Barring of Incoming call supplementary services.* Дополнительные услуги запрета всех входящих звонков.

BIC-Roam – *Barring of Incoming Calls when Roaming outside the home PLMN country supplementary service.* Дополнительная услуга запрета входящих звонков, когда осуществляется роуминг вне страны «домашней» сети PLMN.

Bm – Полноскоростной канал трафика (обмена информацией); обозначение, которое используется в терминологии ISDN для канала передачи информации (речи и данных).

BN – *Bit Number.* Номер бита.

BO – *all Barring of Outgoing call supplementary services.* Дополнительные услуги запрета всех исходящих звонков.

BOIC – *Barring of Outgoing International Calls supplementary service.* Дополнительная услуга запрета исходящих международных звонков.

BOIC-exHC – *Barring of Outgoing International Calls except those directed to the Home PLMN Country supplementary service.* Дополнительная услуга запрета исходящих международных звонков за исключением направленных к стране «домашней» сети PLMN.

BS – *(1) Basic Service (group).* Основное обслуживание (группы).

BS – *(2) Bearer Service.* Служба (обслуживание) передачи информации (данных).

BSG – *Basic Service Group.* Группа основного обслуживания.

BSC – *Base Station Controller.* Контроллер базовой станции.

BSIC – *Base transceiver Station Identity Code.* Код идентификации базовой приемо-передающей станции.

BSIC-NCELL – *BSIC of an adjacent cell.* BSIC соседней соты.

BSS – *Base Station System.* Система базовой станции.

BSSAP – *Base Station System Application Part.* Часть прикладных программ системы базовой станции.

BSSMAP – *Base Station System Management Application Part.* Часть прикладных программ системы управления базовой станции.

BSSOMAP – *Base Station System Operation and Maintenance Application Part.* Часть прикладных программ системы эксплуатации и технического обслуживания базовой станции.

BTS – *Base Transceiver Station.* Базовая приемо-передающая станция.

C

C – *Conditional.* Условный.

CA – *Cell Allocation.* Назначение (размещение) соты.

CAI – *Charge Advice Information.* Информация о состоянии счета (стоимости разговора).

CB – *Cell Broadcast.* Передача сигналов соты.

CBC – *Cell Broadcast Centre.* Центр передачи сигналов соты.

CBCH – *Cell Broadcast CHannel.* Канал передачи сигналов соты.

CBMI – *Cell Broadcast Message Identifier.* Идентификатор передачи сообщения соты.

CC – *(1) Country Code.* Международный код страны.

CC – *(2) Call Control.* Управление вызовом.

CCBS – *Completion of Calls to Busy Subscriber supplementary service.* Дополнительная услуга дозвона до занятого номера абонента.

CCCH – *Common Control CHannel.* Общий канал управления.

CCF – *Conditional Call Forwarding.* Условная переадресация вызова.

CCH – *Control CHannel.* Канал управления.

CCITT – *Comite Consultatif International Telegraphique et Telephonique (The International Telegraph and Telephone Consultative Committee – англ.).* Международный консультативный комитет по телеграфии и телефонии (МККТТ), в настоящее время переименован в ITU.

CCM – *Current Call Meter.* Счетчик текущего вызова.

CCP – *Capability/Configuration Parameter.* Параметр возможность/конфигурация.

CCPE – *Control Channel Protocol Entity.* Сущность (объект) протокола управления каналом.

Cct – *Circuit.* В терминологии ISDN обозначает объединение двух каналов передачи для организации одного двунаправленного канала связи.

CDUR – *Chargeable DURation.* Продолжительность разговора, подлежащая оплате.

CED – *called station identifier.* Идентификатор вызывающей станции.

CEIR – *Central Equipment Identity Register.* Регистр идентичности центрального оборудования.

CEND – *end of charge point.* Окончание оплачиваемого времени разговора.

CEPT – *Conference des administrations Europeennes des Postes et Telecommunications (франц.).* Европейская конференция администраций почт и электросвязи.

CF – *(1) Conversion Facility.* Аппаратура (средства) преобразования информации.

CF – *(2) all Call Forwarding services.* Услуги переадресации всех вызовов.

CFF – *Call Forwarding Flags.* Флаги переадресации вызова.

CFB – *Call Forwarding on mobile subscriber Busy supplementary service.* Дополнительная услуга переадресации вызова мобильного абонента в случае занятого номера.

CFNRc – *Call Forwarding on mobile subscriber Not Reachable supplementary service.* Дополнительная услуга переадресации вызова мобильного абонента в случае недоступности.

CFNRy – *Call Forwarding on No Reply supplementary service.* Дополнительная услуга переадресации вызова в случае отсутствия ответа.

CFU – *Call Forwarding Unconditional supplementary service.* Дополнительная услуга безусловной переадресации вызова.

CHP – *CHarging Point.* Начало отсчета времени оплаты разговора.

CHV – *Card Holder Verification information.* Информация о проверке полномочий владельца карты.

CI – *(1) Cell Identity.* Идентификация соты.

CI – *(2) CUG Index.* Индекс CUG.

CIR (C/I) – *Carrier to Interference Ratio.* Отношение уровня сигнала несущей к уровню помехи (отношение несущая/интерференция).

CKSN – *Ciphering Key Sequence Number.* Число последовательностей ключа шифрования.

CLI – *Calling Line Identity.* Идентификация вызывающей линии.

CLIP – *Calling Line Identification Presentation supplementary service.* Дополнительная услуга представления идентификации вызывающей линии.

CLIR – *Calling Line Identification Restriction supplementary service.* Дополнительная услуга ограничения идентификации вызывающей линии.

CM – *Connection Management.* Управление соединением.

CMD – *CoMmanD.* Команда.

CMM – *Channel Mode Modify.* Изменение (модификация) режима канала.

CNG – *CalliNG tone.* Тональный вызов.

COLI – *COnnected Line Identity.* Идентификация подсоединенной линии.

COLP – *COnnected Line identification Presentation supplementary service.* Дополнительная услуга представления идентификации подсоединенной линии.

COLR – *COnnected Line identification Restriction supplementary service.* Дополнительная услуга ограничения идентификации подсоединенной линии.

COM – *COMplete.* Завершение.

CONNACK – *CONNect ACKnowledgement.* Подтверждение соединения.

C/R – *Command/Response field bit.* Бит поля команда/отклик.

CRC – *Cyclic Redundancy Check (3 bit).* Контроль при помощи циклического избыточного кода (3 бита).

CRE – *Call RE-establishment procedure.* Процедура восстановления вызова.

CSPDN – *Circuit Switched Public Data Network.* Сеть передачи данных общего пользования с коммутацией каналов.

CT – *(1) Call Transfer supplementary service.* Дополнительная услуга передачи (переадресации) вызова.

CT – *(2) Channel Tester.* Измеритель канала.

CT – *(3) Channel Type.* Тип канала.

CTR – *Common Technical Regulation.* Общие технические условия (правила).

CUG – *Closed User Group supplementary service.* Дополнительная услуга закрытой группы пользователей.

CW – *Call Waiting supplementary service.* Дополнительная услуга ожидания (удержания) вызова.

D

DAC – *Digital to Analogue Converter.* Цифро-аналоговый преобразователь (ЦАП).

DB – *Dummy Burst.* Ложный (фиктивный) пакет данных.

DCCH – *Dedicated Control CHannel.* Выделенный канал управления.

DCE – *Data Circuit terminating Equipment.* Оконечное оборудование (линии) передачи данных.

DCF – *Data Communication Function.* Функция (назначение) передачи данных.

DCN – *Data Communication Network.* Сеть передачи данных.

DCS1800 – *Digital Cellular System at 1800MHz.* Цифровая система сотовой связи, работающая в диапазоне 1800 МГц.

DET – *DETach.* Отсоединять, отделять.

DISC – *Disconnect.* Разъединять, выключать.

DL – *Data Link (layer).* Линия передачи данных (уровень передачи данных).

DLCI – *Data Link Connection Identifier.* Идентификация подсоединения линии передачи данных.

DLD – *Data Link Discriminator.* Дискриминатор линии передачи данных.

Dm – Канал управления; в терминологии ISDN, применяемой по отношению к службе мобильной связи, используется для обозначения служебного канала передачи управляющих сигналов.

DMR – *Digital Mobile Radio.* Цифровая мобильная радиослужба.

DNIC – *Data network identifier.* Идентификатор сети передачи данных.

DP – *Dial/Dialled Pulse.* Импульс набора (набираемой цифры).

DRX – *Discontinuous reception.* Прерывистый (скачкообразный) прием сигнала.

DSE – *Data Switching Exchange.* Обмен с коммутацией данных, коммутатор данных.

DSI – *Digital Speech Interpolation.* Цифровая интерполяция речи, статистическое уплотнение речевых сигналов в цифровой форме.

DSS1 – *Digital Subscriber Signalling No1.* Протокол обмена цифровыми сигналами между абонентом и местной сетью (цифровая система сигнализации № 1).

DTAP – *Direct Transfer Application Part.* Часть прикладных программ непосредственной передачи (перевода) обслуживания.

DTE – *Data Terminal Equipment.* Оконечное оборудование (обработки или передачи данных).

DTMF – *Dual Tone Multi-Frequency (signalling).* Двухтональный многочастотный набор телефонного номера (передача сигнализации).

DTX – *Discontinuous transmission.* Прерывистая (скачкообразная) передача сигнала.

E

EA – *External Alarms.* Внешние аварийные сигналы.

EBSG – *Elementary Basic Service Group.* Начальная (элементарная) группа основного обслуживания.

ECM – *Error Correction Mode (facsimile).* Режим исправления ошибок (факсимильных сообщений).

Ec/No – Отношение количества энергии в бите к спектральной плотности потока мощности шумов.

ECT – *Explicit Call Transfer supplementary service.* Дополнительная услуга явной (определенной) передачи (переадресации) вызова.

EEL – *Electric Echo Loss.* Электрические потери на эхо-сигнал.

EIR – *Equipment Identity Register.* Регистр идентификации оборудования.

EL – *Echo Loss.* Потери на эхо-сигнал.

EMC – *ElectroMagnetic Compatibility.* Электромагнитная совместимость.

eMLPP – *enhanced Multi-Level Precedence and Pre-emption service.* Услуга расширенного многоуровневого приоритета и прерывания обслуживания.

EMMI – *Electrical Man Machine Interface.* Электрический человеко-машинный интерфейс.

EPROM – *Erasable Programmable Read Only Memory.* Стираемая программируемая постоянная память (стираемое программируемое постоянное запоминающее устройство).

ERP – *(1) Ear Reference Point.* Исходная (опорная) точка выхода звукового колебания.

ERP – *(2) Equivalent Radiated Power.* Эквивалентная излучаемая мощность (мощность эквивалентного изотропного излучателя).

ERR – *ERRor.* Ошибка.

ETR – *ETSI Technical Report.* Технический отчет ETSI.

ETS – *European Telecommunication Standard.* Европейский стандарт по телекоммуникациям.

ETSI – *European Telecommunications Standards Institute.* Европейский институт стандартов по телекоммуникациям.

Ext – *Extension.* Расширение, добавление.

F

FA – *(1) Full Allocation.* Полное распределение (частот или каналов).

FA – *(2) Fax Adaptor.* Адаптер (переходное устройство) для подключения факсимильного аппарата.

FAC – *Final Assembly Code.* Код (места) окончательной сборки (устройства).

FACCH – *Fast Associated Control CHannel.* Совмещенный канал управления с высокой скоростью передачи информации.

FACCH/F – *Fast Associated Control Channel/Full rate.* Совмещенный канал управления с высокой скоростью передачи информации, работающий в полноскоростном режиме.

FACCH/H – *Fast Associated Control Channel/Half rate.* Совмещенный канал управления с высокой скоростью передачи информации, работающий в полускоростном режиме.

FB – *Frequency correction Burst.* Частотная коррекция пакета данных.

FCCH – *Frequency Correction CHannel.* Частотная коррекция канала.

FCS – *Frame Check Sequence.* Контрольная последовательность (код) кадра; часть кадра, предназначенная для проверки на наличие ошибок в принятом кадре.

FDM – *Frequency Division Multiplex.* Метод уплотнения с частотным разделением каналов.

FDN – *Fixed Dialling Number.* Набор фиксированных номеров.

FEC – *Forward Error Correction.* Предварительная коррекция ошибок.

FER – *(1) Frame Erasure Ratio.* Коэффициент стирания (разрушения) кадра.

FER – *(2) Frame Error Rate.* Вероятность ошибок на кадр.

FH – *Frequency Hopping.* Скачкообразная перестройка по частоте.

FN – *Frame Number.* Номер кадра.

FPLMN – *Forbidden PLMN.* Запрещенные для регистрации сети PLMN.

FR – *Full Rate.* Полная (нормальная) скорость передачи данных.

ftn – *forwarded-to number.* Номер, на который производится переадресация.

G

GCR – *Group Call Register.* Регистр группы вызова.

GID1 – *Group IDentifier level 1.* Идентификатор группы первого уровня.

GMSC – *Gateway Mobile-services Switching Centre.* Межсетевой интерфейс мобильных служб центра коммутации.

GMSK – *Gaussian Minimum Shift Keying (modulation).* Гауссова манипуляция с минимальным сдвигом (метод модуляции).

GPA – *GSM PLMN Area.* Зона PLMN сети GSM.

GPRS –, *General Packet Radio Service.* Служба пакетной передачи данных в радиоканале.

GSA – *GSM System Area.* Зона (обслуживания) системы GSM.

GSM – *Global System for Mobile communications.* Глобальная система мобильной связи.

GSM MS – *GSM Mobile Station.* Мобильная станция системы GSM.

GSM PLMN – *GSM Public Land Mobile Network.* Наземная сеть мобильной связи общего пользования системы GSM.

GT – *Global Title.* Глобальное (общее) название, наименование.

H

HANDO – *HANDOver.* Передача обслуживания.

HDLC – *High level Data Link Control.* Высокоуровневое управление каналом передачи данных.

HLC – *High Layer Compatibility.* Совместимость на высоком уровне.

HLR – *Home Location Register.* Регистр «домашней» сети (база данных, содержащая сведения об абонентах, зарегистрированных в определенной сети).

HOLD – *Call hold supplementary service.* Дополнительная услуга удержания (сохранения) вызова.

HPLMN – *Home PLMN.* «Домашняя» сеть PLMN.

HPU – *Hand Portable Unit.* Ручной переносной блок (устройство).

HR – *Half Rate.* Полускоростной режим передачи данных.

HSN – *Hopping Sequence Number.* Число последовательных перескоков (перестроек) по частоте.

HU – *Home Units.* Бытовые устройства.

I

I – *Information frames (RLP).* Информационные кадры (RLP).

IA – *Incoming Access (closed user group SS).* Доступ входящих вызовов (закрытой группы пользователей SS).

IAM – *Initial Address Message.* Начальный адрес сообщения.

IC – *Interlock Code (CUG SS).* Код блокировки (для CUG SS).

ICB – *Incoming Calls Barred (within the CUG).* Запрет входящих звонков (в пределах CUG).

ICC – *Integrated Circuit(s) Card.* Карта с микросхемой (микропроцессором).

ICCID – *Integrated ChipCard IDentification.* Номер идентификации чип-карты.

IC(pref) – *Interlock Code of the preferential CUG.* Код блокировки предпочтительной CUG.

ICM – *In-Call Modification.* Модификация входящих вызовов.

ID – *IDentification/IDentity/IDentifier.* Идентификация/идентичность/идентификатор.

IDN – *Integrated Digital Network.* Интегральная цифровая сеть связи.

IE – *(signalling) Information Element.* Информационная составляющая (сигнализации).

IEC – *International Electrotechnical Commission.* Международная электротехническая комиссия (МЭК).

IEI – *Information Element Identifier.* Идентификатор информационной составляющей.

I-ETS – *Interim European Telecommunications Standard.* Временный европейский стандарт по телекоммуникациям.

IMEI – *International Mobile station Equipment Identity*. Международный идентификационный номер мобильной станции.

IMSI – *International Mobile Subscriber Identity*. Международный номер идентификации мобильного абонента.

IN – *Interrogating Node*. Узел опроса.

ISC – *International Switching Centre*. Международный коммутационный центр.

ISDN – *Integrated Services Digital Network*. Цифровая сеть с интеграцией услуг.

ISO – *International Organization for Standardization*. Международная организация по стандартизации.

ISUP – *ISDN User Part (of signalling system No.7)*. Часть сети ISDN, относящаяся к пользователю (системы сигнализации № 7).

ITC – *Information Transfer Capability*. Пропускная способность канала передачи информации.

ITU – *International Telecommunication Union*. Международный союз электросвязи (МСЭ).

IWF – *InterWorking Function*. Функция обеспечения межсетевого обмена.

IWMSC – *InterWorking MSC*. Обеспечение межсетевого обмена MSC.

IWU – *InterWorking Unit*. Устройство (блок) межсетевого обмена.

K

K – Ограничение длины сверточного кода.

Kc – *Ciphering key*. Ключ шифрования (криптографический ключ).

Ki – *Individual subscriber authentication key*. Индивидуальный ключ аутентификации абонента.

L

L1 – *Layer 1*. Уровень 1 (физический) в модели взаимодействия открытых систем OSI, определяет связь на уровне аппаратуры.

L2 – *Layer 2*. Уровень 2 (канальный) в модели взаимодействия открытых систем OSI.

L2ML – *Layer 2 Management Link*. Уровень 2 управления каналом связи.

L2R – *Layer 2 Relay*. Уровень 2 (канальный) передачи данных.

L2R BOP – *L2R Bit Orientated Protocol*. Протокол L2R, ориентированный на бит.

L2R COP – *L2R Character Orientated Protocol.* Протокол L2R, ориентированный на символ.

L3 – *Layer 3.* Уровень 3 (сетевой) в модели взаимодействия открытых систем OSI.

LA – *Location Area.* Область (зона) местонахождения.

LAC – *Location Area Code.* Код зоны местонахождения.

LAI – *Location Area Identity.* Идентификация зоны местонахождения.

LAN – *Local Area Network.* Локальная (вычислительная) сеть.

LAPB – *Link Access Protocol Balanced.* Равноправный (сбалансированный) протокол доступа к каналу связи.

LAPDm – *Link Access Protocol on the Dm channel.* Протокол доступа к каналу связи по служебному каналу Dm.

LCN – *Local Communication Network.* Локальная (местная) сеть связи.

LE – *Local Exchange.* Местный коммутатор.

LI – *(1) Length Indicator.* Индикатор длины.

LI – *(2) Line Identity.* Идентификация (опознавание) линии связи.

LLC – *Low Layer Compatibility.* Совместимость на низком уровне.

Lm – Канал трафика (обмена информацией), имеющий пропускную способность ниже пропускной способности канала Bm.

LMSI – *Local Mobile Station Identity.* Локальный (местный) идентификационный номер мобильной станции.

LND – *Last Number Dialled.* Последний набранный номер.

LOCI – *LOCation Information.* Информация о местонахождении.

LP – *Language Preference.* Предпочитаемый язык.

LPLMN – *Local PLMN.* Местная сеть PLMN.

LR – *Location Register.* Регистр местонахождения.

LSTR – *Listener SideTone Rating.* Допустимый уровень самопрослушивания (местный эффект) приемной стороны.

LTE – *Local Terminal Emulator.* Местный эмулятор терминала (оконечного устройства).

LU – *(1) Local Units.* Местные единицы (расчета).

LU – *(2) Location Update.* Обновление данных о местонахождении (мобильной станции).

LV – *Length and Value.* Длина и значение.

M

M – *Mandatory.* Обязательный.

MA – *Mobile Allocation.* Мобильное размещение.

MACN – *Mobile Allocation Channel Number.* Число каналов мобильного размещения.

MAF – *Mobile Additional Function.* Добавочное (дополнительное) мобильное назначение.

MAH – *Mobile Access Hunting supplementary service.* Дополнительная услуга поиска мобильного доступа (к сети).

MAI – *Mobile Allocation Index.* Индекс мобильного размещения.

MAIO – *Mobile Allocation Index Offset.* Индекс перемещения (изменения местоположения) мобильного размещения.

MAP – *Mobile Application Part.* Часть прикладных программ мобильной станции.

MCC – *Mobile Country Code.* Международный код страны в сети мобильной связи.

MCI – *Malicious Call Identification supplementary service.* Дополнительная услуга идентификации вызова злоумышленника.

MD – *Mediation Device.* Прибор-посредник; устройство, используемое на станции для подсоединения оконечного оборудования данных к передающей среде.

MDL – *(mobile) Management (entity) – Data Link (layer).* Объект мобильного управления – канал передачи данных (уровень).

ME – *(1) Maintenance Entity.* Техническое обслуживание объекта.

ME – *(2) Mobile Equipment.* Мобильное оборудование.

MEF – *Maintenance Entity Function.* Назначение технического обслуживания объекта.

MF – *MultiFrame.* Мультикадр (группа кадров).

MHS – *Message Handling System.* Система обработки (управления) сообщений.

MIC – *Mobile Interface Controller.* Контроллер мобильного интерфейса.

MM – *(1) Man Machine.* Интерфейс «человек-машина».

MM – *(2) Mobility Management.* Управление мобильностью.

MME – *Mobile Management Entity.* Объект мобильного управления.

MMI – *Man Machine Interface.* Человеко-машинный интерфейс.

MNC – *Mobile Network Code.* Код сети мобильной связи.

MO – *Mobile Originated.* Исходящий от мобильной станции (вызов).

MoU – *Memorandum of Understanding.* Меморандум о взаимопонимании; документ, подписанный в сентябре 1987 года операторами сети GSM из 13 европейских стран.

MPH – *(mobile) Management (entity) – PHysical (layer) [primitive].* Объект мобильного управления – физический уровень (первичный).

MPTY – *MultiParTY (Multi ParTY) supplementary service.* Дополнительная услуга конференц-связи.

MRP – *Mouth Reference Point.* Исходная (опорная) точка входа звукового колебания.

MS – *Mobile Station.* Мобильная станция.

MSC – *Mobile-services Switching Centre, Mobile Switching Centre.* Центр коммутации мобильной связи.

MSCM – *Mobile Station Class Mark.* Марка класса мобильной станции.

MSCU – *Mobile Station Control Unit.* Блок управления мобильной станции.

MSISDN – *Mobile Station International ISDN Number.* Международный номер ISDN мобильной станции.

MSRN – *Mobile Station Roaming Number.* Номер мобильной станции в роуминге.

MT – *Mobile Terminated.* Подсоединенная мобильная станция.

MTM – *Mobile-To-Mobile (call).* Вызов с одного мобильного телефона на другой мобильный.

MTP – *Message Transfer Part.* В системе передачи сообщений часть сигнала, содержащая собственно сообщение.

MU – *Mark Up.* Записывать на счет.

MUMS – *Multi User Mobile Station.* Многоабонентская (многопользовательская) мобильная станция.

N

N/W – *Network.* Сеть.

NB – *Normal Burst.* Обычный (стандартный) пакет данных.

NBIN – Параметр, используемый в последовательности перескоков по частоте.

NCC – *Network (PLMN) Colour Code.* Цветовой код сети (PLMN).

NCELL – *Neighbouring (of current serving) Cell.* Соседняя сота (текущего обслуживания).

NCH – *Notification CHannel.* Канал уведомления (предупреждения).

NDC – *National Destination Code.* Национальный код места назначения (приемной стороны).

NDUB – *Network Determined User Busy.* Сеть, установленная (определенная) пользователем в случае занятого номера.

NE – *Network Element.* Элемент (составляющая) сети.

NEF – *Network Element Function.* Назначение элемента сети.

NET – *Norme Europeenne de Telecommunications (франц.).* Европейский стандарт по телекоммуникациям.

NF – *Network Function.* Назначение сети.

NIC – *Network Independent Clocking.* Сеть с независимой синхрони-

NM – *Network Management.* Управление сетью.

NMC – *Network Management Centre.* Центр управления сетью.

NMSI – *National Mobile Station Identification number.* Национальный идентификационный номер мобильной станции.

NPI – *Number Plan Indentifier.* Идентификатор номера (тарифного) плана.

NSAP – *Network Service Access Point.* Точка доступа к сетевому обслуживанию.

NT – *(1) Network Termination.* Оконечное оборудование сети.

NT – *(2) Non Transparent.* Непрозрачность.

NTAAB – *New Type Approval Advisory Board.* Консультативный комитет по подтверждению новых типов.

NUA – *Network User Access.* Доступ пользователя к сети.

NUI – *Network User Identification.* Идентификация пользователя сети.

NUP – *National User Part (SS7).* Часть национальной сети (системы SS7), относящаяся к пользователю.

O

O – *Optional.* Возможный (факультативный).

OA – *Outgoing Access (CUG SS).* Доступ исходящих вызовов (для CUG SS).

O&M – *Operations & Maintenance.* Эксплуатация и техническое обслуживание.

OACSU – *Off-Air-Call-Set-Up.* Установка соединения по вызову, принимаемому непосредственно из эфира.

OCB – *Outgoing Calls Barred within the CUG.* Запрет исходящих звонков в рамках CUG.

OLR – *Overall Loudness Rating.* Общий допустимый уровень громкости.

OMC – *Operations & Maintenance Centre.* Центр эксплуатации и технического обслуживания.

OML – *Operations and Maintenance Link.* Канал эксплуатации и технического обслуживания.

OS – *Operating System.* Операционная система.

OSI – *Open System Interconnection.* Протокол взаимодействия открытых систем.

OSI RM – *OSI Reference Model.* Модель взаимодействия открытых систем OSI (семиуровневая иерархическая модель, разработанная Международным комитетом по стандартизации OSI для определения спецификации и связи сетевых протоколов).

P

PABX – *Private Automatic Branch eXchange.* Частная (офисная) АТС с исходящей и входящей связью.

PAD – *Packet Assembly/Disassembly facility.* Средства (аппаратура) сборки/разборки пакетов данных.

PCH – *Paging CHannel.* Канал передачи системы персонального вызова.

PCM – *Pulse Code Modulation.* Импульсно-кодовая модуляция (ИКМ).

PD – *(1) Protocol Discriminator.* Протокольный дискриминатор.

PD – *(2) Public Data.* Данные общего пользования.

PDN – *Public Data Networks.* Сеть передачи данных общего пользования.

PH – *(1) Packet Handler.* Обработчик (программа обработки) пакетов данных.

PH – *(2) PHysical (layer).* Физический (первый) уровень взаимодействия OSI.

PHI – *Packet Handler Interface.* Интерфейс устройства обработки пакетов данных.

PI – *Presentation Indicator.* Индикатор представления.

PICS – *Protocol Implementation Conformance Statement.* Протокол реализации соответствующего предложения.

PIN – *Personal Identification Number.* Личный (персональный) идентификационный номер.

PIXT – *Protocol Implementation eXtra information for Testing.* Протокол реализации дополнительной информации для тестирования.

PLMN – *Public Lands Mobile Network.* Наземная сеть мобильной связи общего пользования.

POI – *Point Of Interconnection (with PSTN).* Точка взаимодействия с PSTN.

PP – *Point-to-Point.* Непосредственное (прямое) соединение между двумя интерфейсами (типа «точка-точка»).

PPE – *Primitive Procedure Entity.* Объект (сущность) первичной (элементарной) процедуры.

Pref CUG – *Preferential CUG.* Предпочтительная CUG.

Ps – Вероятность местонахождения.

PSPDN – *Packet Switched Public Data Network.* Сеть передачи данных общего пользования с пакетной коммутацией.

PSTN – *Public Switched Telephone Network.* Коммутируемая телефонная сеть общего пользования.

PUCT – *Price per Unit Currency Table.* Таблица цен за расчетную единицу.

PW – *Pass Word.* Код доступа (пароль).

Q

QA – *Q (Interface) – Adapter.* Интерфейс-адаптер.

QAF – *Q – Adapter Function.* Функция интерфейс-адаптер.

QOS – *Quality Of Service.* Качество и класс предоставляемых услуг.

R

R – Величина, на которую снижается ВЧ мощность, передаваемая мобильной станцией, по отношению к максимально-допустимой выходной мощности мобильной станции самого высокого класса мощности (A).

RA – *RAndom mode request information field.* Произвольный режим запроса информационного поля.

RAB – *Random Access Burst.* Пакет данных произвольного доступа.

RACH – *Random Access CHannel.* Канал с произвольным доступом.

RAND – *RANDom number.* Случайное число (используется при аутентификации мобильной станции).

RBER – *Residual Bit Error Ratio.* Коэффициент необнаруженных (остаточных) ошибок на бит.

RDI – *Restricted Digital Information.* Цифровая информация с ограниченным доступом.

REC – *RECommendation.* Рекомендация (документ).

REJ – *REJect(ion).* Отклонение (запроса), отказ (от выполнения команды).

REL – *RELease.* Разъединять.

REQ – *REQuest.* Запрос.

RF – *Radio Frequency.* Радиочастота, высокая частота (ВЧ).

RFC – *Radio Frequency Channel.* Канал ВЧ.

RFCH – *Radio Frequency CHannel.* Канал ВЧ.

RFN – *Reduced TDMA Frame Number.* Сокращение числа кадров TDMA.

RFU – *Reserved for Future Use.* Зарезервировано для будущего использования.

RLP – *Radio Link Protocol.* Протокол передачи данных радиоканала.

RLR – *Receiver Loudness Rating.* Номинальный (допустимый) уровень громкости приемника.

RMS – *Root Mean Square (value).* Среднеквадратическое, действующее (значение).

RNTABLE – Таблица 128 целых чисел, использующихся в последовательности перескоков по частоте.

RPOA – *Recognised Private Operating Agency.* Общепризнанная частная эксплуатационная служба.

RR – *Radio Resource.* Радиоресурс.

RSE – *Radio System Entity.* Объект (сущность) радиосистемы.

RSL – *Radio Signalling Link.* Радиоканал сигнализации.

RSZI – *Regional Subscription Zone Identity.* Идентичность зоны региональной подписки (абонемента).

RTE – *Remote Terminal Emulator.* Эмулятор удаленного терминала.

RXLEV – *Received signal Level.* Уровень принимаемого сигнала.

RXQUAL – *Received signal Quality.* Качество принимаемого сигнала.

S

S/W – *Software.* Программное обеспечение.

SABM – *Set Asynchronous Balanced Mode.* Установка асинхронного равноправного режима.

SACCH – *Slow Associated Control CHannel.* Совмещенный канал управления с низкой скоростью передачи информации.

SACCH/C4 – *Slow Associated Control CHannel/SDCCH/4.* Совмещенный канал управления с низкой скоростью передачи информации/ SDCCH/4.

SACCH/C8 – *Slow Associated Control CHannel/SDCCH/8.* Совмещенный канал управления с низкой скоростью передачи информации/ SDCCH/8.

SACCH/T – *Slow Associated Control CHannel/Traffic channel.* Совмещенный канал управления с низкой скоростью передачи информации/канал трафика.

SACCH/TF – *Slow Associated Control CHannel/Traffic channel Full rate.* Совмещенный канал управления с низкой скоростью передачи информации/канал трафика, работающий в полноскоростном режиме.

SACCH/TH – *Slow Associated Control CHannel/Traffic channel Half rate.* Совмещенный канал управления с низкой скоростью передачи информации/канал трафика, работающий в полускоростном режиме.

SAP – *Service Access Point.* Точка доступа к услугам.

SAPI – *Service Access Point Indicator.* Индикатор точки доступа к услугам.

SB – *Synchronization Burst.* Сигнал синхронизации пакетов данных.

SC – *(1) Service Centre.* Сервисный центр (используется для передачи SMS-сообщений).

SC – *(2) Service Code.* Код службы.

SCCP – *Signalling Connection Control Part.* Часть информации сигнализации, касающаяся управления соединением.

SCH – *Synchronization CHannel.* Канал синхронизации.

SCN – *Sub-Channel Number.* Номер подканала.

SDCCH – *Stand-alone Dedicated Control CHannel.* Автономный канал, выделенный для управления.

SDL – *Specification Description Language.* Язык описания спецификаций.

SDT – *SDL Development Tool.* Инструментальные средства разработки SDL.

SDU – *Service Data Unit.* Сервисный блок данных, блок обработки эксплутационных данных.

SE – *Support Entity.* Обслуживание (поддержка) объекта.

SEF – *Support Entity Function.* Назначение обслуживания объекта.

SFH – *Slow Frequency Hopping.* Медленные перескоки по частоте.

SI – *(1) Screening Indicator.* Вывод индикации на экран.

SI – *(2) Service Interworking.* Служба межсетевого обмена.

SI – *(3) Supplementary Information (SIA – Supplemenatary Information A).* Дополнительная информация (SIA – дополнительная информация A).

SID – *SIlence Descriptor.* Дескриптор (описатель) пауз.

SIM – *Subscriber Identity Module.* Модуль идентификации абонента.

SIM-Lock – *SIM Locking.* Блокировка (запрет) подключения другой SIM-карты; способ «запирания» (кодирования) мобильного телефона, делающий невозможным его использование с SIM-картой другого оператора.

SLR – *Send Loudness Rating.* Номинальный уровень передаваемой громкости.

SLTM – *Signalling Link Test Message.* Тестовое (контрольное) сообщение канала сигнализации.

SME – *Short Message Entity.* Элемент (компонент) короткого сообщения.

SMG – *Special Mobile Group.* Специальная группа мобильных станций.

SMS – *Short Message Service.* Услуга (служба) передачи коротких сообщений.

SMSCB – *Short Message Service Cell Broadcast.* Услуга передачи коротких сообщений в пределах соты.

SMS-SC – *Short Message Service – Service Centre.* Сервисный центр службы передачи коротких сообщений.

SMS/PP – *Short Message Service/Point-to-Point.* Услуга передачи коротких сообщений при непосредственном соединении (типа «точка-точка»).

Smt – *Short message terminal.* Терминал (оконечное устройство), посылающий или принимающий короткие сообщения.

SN – *Subscriber Number.* Номер абонента.

SNR – *Serial NumbeR.* Серийный номер (устройства или изделия).

SOA – *Suppress Outgoing Access (CUG SS).* Запрет доступа к передаче исходящих сообщений (в CUG SS).

SP – *(1) Service Provider.* Служба провайдера.

SP – *(2) Signalling Point.* Точка сигнализации.

SP – *(3) Spare.* Свободный, резервный.

SPC – *Signalling Point Code.* Код точки сигнализации.

SPC – *Suppress Preferential CUG.* Запрет предпочтительной CUG.

SPN – *Service Provider Name.* Наименование службы провайдера.

SRES – *Signed RESponse.* Полученная подпись (зашифрованная цифровая последовательность) при ответе (в процессе аутентификации).

SS – *(1) Supplementary Service.* Дополнительная услуга.

SS – *(2) System Simulator.* Системный имитатор.

SSC – *Supplementary Service Control string.* Строка управления дополнительными услугами.

SSN – *Sub-System Number.* Номер подсистемы.

SST – *SIM Service Table.* Таблица услуг, оказываемых по SIM-карте.

SS7 – *Signalling System No. 7.* Система сигнализации № 7, используется для установления и управления соединениями в общем канале связи телекоммуникационной сети.

STMR – *SideTone Masking Rating.* Номинальный уровень маскировки самопрослушивания (местного эффекта).

STP – *Signalling Transfer Point.* Точка передачи сигнализации.

SVN – *Software Version Number.* Номер версии программного обеспечения.

T

T – *(1) Timer.* Таймер.

T – *(2) Transparent.* Прозрачность (системы).

T – *(3) Type only.* Только тип.

TA – *Terminal Adaptor.* Терминальный адаптер.

TAC – *Type Approval Code.* Код подтверждения типа.

TAP – *Terminal Adaptation Function.* Назначение терминального адаптера.

TBR – *Technical Basis for Regulation.* Основные технические условия (регламент).

TC – *Transaction Capabilities.* Возможности обработки запросов (трансакций).

TCH – *Traffic Channel.* Канал трафика (информационного обмена).

TCH/F – *A full rate TCH.* Полноскоростной TCH.

TCH/F2,4 – *A full rate data TCH (2,4kbit/s).* Полноскоростной TCH данных (2,4 Кбит/с).

TCH/F4,8 – *A full rate date TCH (4,8kbit/s).* Полноскоростной TCH данных (4,8 Кбит/с).

TCH/F9,6 – *A full rate data TCH (9,6kbit/s).* Полноскоростной TCH данных (9,6 Кбит/с).

TCH/FS – *A full rate Speech TCH.* Полноскоростной TCH речи.

TCH/H – *A half rate TCH.* Полускоростной TCH.

TCH/H2,4 – *A half rate data TCH (2,4kbit/s).* Полускоростной TCH данных (2,4 Кбит/с).

TCH/H4,8 – *A half rate data TCH (4,8kbit/s).* Полускоростной TCH данных (4,8 Кбит/с).

TCH/HS – *A half rate Speech TCH.* Полускоростной TCH речи.

TCI – *Transceiver Control Interface.* Интерфейс управления трансивером (приемо-передатчиком).

TC-TR – *Technical Committee Technical Report.* Технический отчет технического комитета.

TDMA – *Time Division Multiple Access.* Метод многостанционного доступа с временным разделением каналов.

TE – *Terminal Equipment.* Оконечное (терминальное) оборудование.

Tei – *Terminal endpoint identifier.* Идентификатор конечной точки терминала.

TFA – *TransFer Allowed.* Разрешенная передача (обслуживания).

TFP – *TransFer Prohibited.* Запрещенная передача (обслуживания).

TI – *Transaction Identifier.* Идентификатор трансакции (обработки запроса).

TLV – *Type, Length and Value.* Тип, длина и значение.

TMN – *Telecommunications Management Network.* Сеть управления телекоммуникациями.

TMSI – *Temporary Mobile Subscriber Identity.* Временная идентификация (идентификационный номер) мобильного абонента.

TN – *Timeslot Number.* Номер временного интервала (слота).

TON – *Type Of Number.* Тип номера.

TRX – *Transceiver.* Трансивер (приемо-передатчик).

TS – *(1) Time Slot.* Временной интервал (слот) в TDMA.

TS – *(2) Technical Specification.* Техническая характеристика (спецификация).

TS – *(3) TeleService.* Обслуживание удаленных пользователей в соответствии с соглашением между операторами связи.

TSC – *Training Sequence Code.* Код обучающей последовательности.

TSDI – *Transceiver Speech & Data Interface.* Трансивер (приемо-передатчик) речи/интерфейс данных.

TTCN – *Tree and Tabular Combined Notation.* Комбинированное представление в древовидной и табличной форме.

TUP – *Telephone User Part (SS7).* Часть системы сигнализации (SS7), касающаяся пользователя телефона.

TV – *Type and Value.* Тип и значение.

TXPWR – *Transmit PoWeR.* Передача мощности; уровень мощности передатчика при отправке запроса мобильной станцией и при конфигурировании ее параметров.

U

UDI – *Unrestricted Digital Information.* Цифровая информация с неограниченным допуском.

UDUB – *User Determined User Busy.* Пользователь, номер которого определен как занятый.

UI – *Unnumbered Information (Frame).* Ненумерованная (нешифрованная) информация (кадр).

UIC – *Union Internationale des Chemins de Fer (франц.).* Международный железнодорожный союз.

UPCMI – *Uniform PCM Interface (13-bit).* Унифицированный PCM интерфейс (13 бит).

UPD – *Up to date.* Современный, новейший.

USSD – *Unstructured Supplementary Service Data.* Неструктурированные данные дополнительной услуги.

UUS – *User-to-User Signalling supplementary service.* Дополнительная услуга передачи сигнала от пользователя другому пользователю.

V

V – *Value only.* Только значение.

VAD – *Voice Activity Detection.* Детектирование активности речи (наличие сигнала в момент разговора и отсутствие его в паузах).

VAP – *Videotex Access Point.* Точка доступа к системе видеотекса (видеографии).

VBS – *Voice Broadcast Service.* Услуга передачи голосовых сообщений.

VGCS – *Voice Group Call Service.* Услуга голосового вызова группы.

VLR – *Visitor Location Register.* «Гостевой» регистр, регистр перемещений (база данных, содержащая информацию о «гостевых» абонентах).

VMSC – *Visited MSC.* «Гостевой» MSC.

VMWI – *Voice Mail Waiting Indicator.* Индикатор ожидания голосовой почты.

VPLMN – *Visited PLMN.* «Гостевая» сеть PLMN.

VSC – *Videotex Service Centre.* Центр обслуживания системы видеотекс (интерактивной видеографии).

V(SD) – *Send state variable.* Передача переменной состояния.

VTX – *host The components dedicated to Videotex service.* Компоненты хоста (ведущего узла), выделенные для обслуживания системы видеотекса.

W

WS – *Work Station.* Рабочая станция.

WPA – *Wrong Password Attempts (counter).* Число неудачных попыток ввода пароля (счетчик).

X

XID – *eXchange IDentifier.* Идентификатор коммутатора.

Z

ZC – *Zone Code.* Код зоны.

6.2. МЕЖДУНАРОДНЫЙ РОУМИНГ КОМПАНИИ SWISSCOM MOBILE

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Австралия	505	03	Vodafone PTY	+61 414–416	15.07.1994
Австралия	505	02	Optus	+61 411–413	23.09.1994
Австралия	505	01	Telecom Australia (Telstra)	+61 417–419	15.07.1994
Австрия	232	01	Mobilkom	+43 664	15.02.1994
Австрия	232	03	Max Mobilkom	+43 676	14.10.1996
Азербайджан	400	01	Azercell	+994 50	24.02.1997
Азербайджан	400	02	Bakcell	+994 55	09.06.1999
Албания	276	01	AMC	+355 38	29.04.1998
Алжир	603	01	MPTT	+213 01	20.10.2000
Андорра	213	03	STA	+376 75	10.07.1995
Бангладеш	470	01	Grameen Phone Limited	+880 17	23.09.1999
Бахрейн	426	01	Bahrain Batelco	+973 96	15.07.1996
Беларусь	257	01	MDC (Mobile Digital Comm.)	+375 296	13.09.1999
Бельгия	206	01	Belgacom	+32 75	01.07.1994
Бельгия	206	10	Mobilstar	+32 95	14.10.1996
Болгария	284	01	MobTel AD	+359 88	12.02.1996
Босния и Герцеговина	218	90	BIH	+387 90	28.01.1998
Босния и Герцеговина	218	03	Eronet	+387 663	24.10.2000
Босния и Герцеговина	218	05	Mobilna Srpske	+387 66	14.12.2000
Ботсвана	652	01	Mascom	+267 71	21.09.1999
Ботсвана	652	02	Vista Cellular	+267 7	19.02.2000
Бруней	528	11	DST Communications Br.	+678 8	22.09.1997
Ватикан			Telecom Italia или Omnitel		
Великобритания	234	10	Cellnet Securicor	+44 802	11.07.1994
Великобритания, остров Мэн (графство)	234	58	Manx Telecom	+44 4624	15.07.1996
Великобритания, остров Джерси (графство)	234	50	Jersey Telecom	+44 97	31.12.1994
Великобритания	234	15	Vodafone	+44 385	02.08.1993
Венгрия	216	01	Pannon	+36 20	11.07.1994
Венгрия	216	70	Vodafone	+36 70	30.11.1999
Венгрия	216	30	Westel 900	+36 30	18.04.1994
Венесуэла	404	07	Digitel	+58 12	23.11.1999
Вьетнам	452	01	VMS MobiFone	+84 90	07.04.2000

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (продолжение)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Вьетнам	452	02	VinaPhone GSM	+84 91	05.01.2001
Гвиана Французская	340	01	FCM (Guy. Franc.)	+590 35	10.12.1999
Гана	620	01	Scancom	+233 24	02.03.2002
Гваделупа	340	01	FCM (Guadeloupe)	+590 35	10.12.1999
Германия	262	01	D1 DeTeMobil	+49 171	01.01.1993
Германия	262	02	D1 Manesmann	+49 172	15.12.1992
Гернси	234	55	Guernsey Telecom	+44 4481	02.05.1996
Гибралтар	266	01	Gibtel	+350 58	01.06.1995
Гонконг	454	06	SmarTone	+852 901	20.06.1994
Гонконг	454	04	Hong Kong Hutchison	+852 904	30.04.1996
Гонконг	454	00	Cable Wireless	+852 902+909	16.01.1995
Гренландия	290	01	TELE Greenland	+299 49, 52-55, 59	08.03.2000
Греция	202	05	Panafon	+30 94	14.02.1994
Греция	202	10	STET Hellas	+30 93	13.06.1994
Грузия	282	02	Magticom Ltd.	+995 32	19.02.1998
Грузия	282	01	Geocell Georgia	+995 77	08.09.1997
Дания	238	02	Dansk Mobil Telefon Sonofon	+45 405	18.11.1992
Дания	238	01	TeleDenmark Mobil	+45 401–403	01.11.1992
Египет	602	01	MobiniI	+20 12	15.10.1998
Египет	602	02	MisrFone	+20 10	30.11.1998
Зимбабве	648	01	NetOne	+263 11	07.12.1998
Зимбабве	648	03	Telecel	+263 23	23.11.2000
Зимбабве	648	04	Econet	+263 91	01.04.1999
Израиль	425	01	Parther Communications	+972 54	17.12.1998
Индия (Бангалор, Хайдарабад)	404	45/49	JTM	+91 9845	01.07.1999
Индия (Гуджарат)	404	05	Facsel	+91 9825	15.03.1999
Индия (Гуджарат)	404	24	Birla AT&T	+91 9824	27.01.2000
Индия (Дели)	404	10	Airtel Barthi India	+91 981	28.09.1998
Индия (Дели)	404	11	Sterling Cellular (Essar)	+91 9811	26.08.1998
Индия (Калькутта)	404	30	Usha Martin	+91 9830	09.12.1998
Индия (Калькутта)	404	31	Modi Telstra	+91 9831	24.12.1999
Индия (Карнатака)	404	44	Spice Communications	+91 98440	24.03.2000
Индия (Мадрас)	404	41	RPG Cellular Services Ltd.	+91 9841	25.06.1999
Индия (Мадрас)	404	40	Skycell	+91 9840	26.03.1999

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (продолжение)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Индия (Мамбаи)	404	20	Hutchison Max Telecom	+91 9820	15.12.1998
Индия (Мамбаи)	404	21	BPL Mobile Communication	+91 9821	07.03.1999
Индия (Махараштра)	404	22	Birla AT&T	+91 9822	05.04.2000
Индия (Махараштра)	404	46/43/27	BPL Cellular	+91 9846, +91 9843, +91 9823	10.02.2000
Индия (Пенджаб)		14	Spice Telecom Punjab	+91 9814	05.12.2000
Индия (Раджастхан)	404	70	Hexacom	+91 9829	13.10.1999
Индия (Хайдарабад)	404	07	Tata Communications	+91 9848	23.11.1999
Индия	404	12	Escotel Haryana	+91 9812	05.12.2001
Индия	404	19	Escotel Kerala	+91 9847	28.03.2001
Индия	404	56	Escotel Up West	+91 98370	21.12.2000
Индонезия	510	00	Pasific Satelit Nusantara	+62 8681	01.06.2000
Индонезия	510	01	PT Satelit Palapa Ind.	+62 816	12.03.1996
Индонезия	510	10	Telekomunikasi (Telkomsel)	+62 811	02.09.1996
Индонезия	510	11	Excelcomindo	+62 818	18.03.1997
Иордания	416	01	Fastlink	+962 79	08.08.1997
Иордания	416	77	MobileCom	+962 77	02.11.2000
Ирландия	272	01	Eircell	+353 87	01.02.1994
Ирландия	272	02	Esat Digifone	+353 89	03.03.1997
Исландия	274	01	Landssiminn	+354 89	15.11.1994
Исландия	274	02	TAL Ltd	+354 69	22.07.1998
Испания	214	07	Telefonica Moviles	+34 609	14.07.1995
Испания	214	01	Airtel Movil	+34 07	02.10.1995
Италия	222	10	Omnitel - Vodafone	+39 34	01.10.1995
Италия	222	01	Telecom Italia	+39 33, 35, 39)	01.01.1993
Италия	222	88	Wind	+39 320	01.03.1999
Казахстан	401	02	K'Cell GSM	+7 300	05.07.1999
Казахстан	401	01	K-Mobile Kar Tel	+7 333	23.06.1999
Камбоджа	456	01	CamGSM	+855 12	14.12.1998
Камбоджа	456	02	Casacom	+855 16	06.10.2000
Камерун	624	02	SCM Soc. Cam. de Mob.	+237 9	03.04.2001
Катар	427	01	Q-Tel	+974 5	01.06.1995
Кения	254	73	Kencell	+63903	18.01.2001
Кипр	280	01	CYTA	+357 9	07.08.1995
Китай	460	00	Chine Mobile	+86 139	21.04.1997
Китай	460	01	Chine Unicom	+86 130	25.06.1999
Кот-д'Ивуар	612	03	SIM Ivoirus	+225 07	18.05.1998

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (продолжение)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Кот-д'Ивуар	612	05	Loteny Telecom	+225 05	09.03.1998
Косово	212	01	Monaco Tel. (Vala)	+377 44	09.05.2000
Кувейт	419	02	MTC	+965 96	01.08.1995
Кувейт	419	03	Wataniya Telecom	+965 6	10.01.00
Кыргызстан	437	01	Bitel	+996 502	10.05 99
Латвия	247	01	LMT	+371 92	10.04.1995
Латвия	247	02	Baltcom GSM	+371 95	29.10.1997
Ливан	415	01	FTML Lebanon	+961 34	23.09.1996
Ливан	415	03	Libancell Lebanon	+961 37	12.09.1996
Литва	246	02	Bite GSM	+370 99	25.04.1996
Литва	246	01	Omnitel Lithuania	+370 98	01.08.1996
Лихтенштейн	228	01	Swisscom	+41 79	
Лихтенштейн	270	77	Tango	+423 76	24.03.2000
Люксембург	270	01	P&T Luxembourg	+352 21	01.07.1993
Люксембург	270	77	Millcom/Tango	+352 091	18.09.1998
Маврикий	617	01	Cellplus	+230 25	06.06.1996
Маврикий	617	10	Emtel	+230 72	15.06.2000
Мадагаскар		01	Madacom SA	+261 33	16.08.1999
Макао	455	01	CTM	+853 68	15.03.1996
Македония	294	01	Mobimak	+389 70	01.07.1997
Малайзия	502	19	Celcom Malaysia	+60 19	07.10.1996
Малайзия	502	12	Maxis (Binariang)	+60 12	20.05.1996
Мальдивы	472	01	Dhiraagu	+960 77, 78, 79	03.10.2000
Мальта	278	01	Vodafone	+356 94	19.08.1997
Марокко	604	00	Meditelecom	+212 3+4	28.07.2000
Марокко	604	01	ONPT	+212 213	27.03.1995
Мартиника	340	01	FCM (Martinique)	+590 35	10.12.1999
Мозамбик	643	01	TDM	+258 82	22.09.1999
Молдова	259	01	Voxtel SA	+373 91	22.02.1999
Молдова	259	02	Moldcell	+373 94	12.09.2000
Намибия	649	01	MTC Namibia	+264 81	01.10.1996
Нидерланды	204	04	Libertel	+31 654	01.02.1996
Нидерланды	204	08	Telecom PTT	+31 653	01.07.1994
Новая Зеландия	530	01	Vodafone N.Z. (Bell N.Z.)	+64 21	15.10.1996
Норвегия	242	01	Telenor Mobil	+47 900	01.11.1992
Норвегия	242	02	Netcom GSM	+47 920	01.10.1993
Объединенные Арабские Эмираты	424	02	Etisalat	+971 50	11.11.1994
Оман	422	02	GTO Ministry of PTT	+968	29.09.1997
Острова Зеленого Мыса	625	01	Cabo Verde Telecom	+238 91	27.04.2001
Пакистан	410	01	PMC Mobilink	+92 300	16.11.1998
Палестинская автономия	425	05	Paltel	+972 59	08.10.1999
Польша	260	01	Polcom Tel	+48 601	04.11.1996

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (продолжение)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Польша	260	02	Polska Telefonia Cyfrowa	+48 602	06.12.1996
Португалия	268	01	Telecel	+351 931	29.07.1993
Португалия	268	05	Telemovel	+351 936	01.07.1993
Реюньон (остров)	647	10	SRR, Sosiete Reun. du Radio	+262	05.08.1998
Россия (Москва)	250	01	Мобильные ТелеСистемы (МТС), Москва (MTS Moscow)	+7 095	01.02.1996
Россия (Санкт-Петербург)	250	02	Северо-Западный GSM (North-West GSM)	+7 812	15.03.1996
Россия (Екатеринбург)	250	39	Уралтел (Uraltel Ltd.)	+7 343	10.07.1998
Россия (Калининград)	250	28	Экстел (Extel)	+7 0119	25.10.1999
Россия (Краснодар)	250	13	Кубань GSM (Kuban GSM)	+7 90243	01.10.1998
Россия (Нижний Новгород)	250	03	Нижегородская сотовая связь (NCC)	+7 90270	01.10.1999
Россия (Новосибирск)	250	05	Сибирские сотовые системы (Siberian Ceccular Systems)	+7 902 98	26.04.1999
Россия (Ростов)	250	10	Донтелеком (DonTelecom)	+7 90245	12.10.1998
Россия (Самара)	250	07	СМАРТС (Zao Smarts)	+7 902370	02.03.1999
Россия (Ставрополь)	250	44	Телесот-Ставрополь (StavTeleSot)	+7 865	01.06.1999
Россия	250	12	Дальневосточные сотовые системы (Far-Eastern)	+7 902 403	01.02.2000
Россия	250	17	Ermak	+7 346	07.12.2000
Россия	250	16	NTC New Teleph. Comp.	+7 902	29.01.2001
Румыния	226	10	Mobilrom	+40 94	30.06.1997
Румыния	226	01	Mobifon	+40 92	12.08.1997
Сан-Марино			Telecom Italia или Omnitel		
Саудовская Аравия	420	01	MOPTT	+966 55	30.06.1997
Саудовская Аравия	420	07	EAE Aljawwal	+966 1299	11.01.1999
Сейшельские острова	633	01	Cable & Wireless	+248 51	09.09.1998

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (продолжение)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Сейшельские острова	633	10	Airtel Telecom Ltd.	+248 7	27.07.1999
Сенегал	608	02	Sentel	+221 68	02.02.00
Сенегал	608	01	Sonantel Alize	+221 63	23.02.1998
Сингапур	525	03	MobileOne	+65 9	24.03.1997
Сингапур	525	01	Singapore Telecom	+65 15	15.10.1994
Словакия	231	01	Globtel Slovakia	+421 905	14.04.1997
Словакия	231	02	Eurotel Bratislava	+421 903	14.04.1997
Словения	293	41	Mobitel	+386 41	14.10.1996
Словения	293	40	SLMobil	+386 40	26.04.1999
Судан	643	01	Mobitel	+249 12	01.09.1999
Таиланд	520	01	AIS	+66 1	15.09.1995
Тайвань	466	99	TransAsia Telecoms	+886 931	26.05.1998
Тайвань	466	93	Mobitai Communications	+886 9316	01.04.1998
Тайвань	466	92	Chunghwa (LTDA)	+886 92	01.02.1996
Танзания	640	01	Tritel	+855 812	06.02.1998
Танзания	640	04	Vodacom Ltd	+255 744	28.05.2001
Того	228	04/05	Togo Cellulaire	+01	26.08.1999
Тунис	605	02	Tunicell	+216 9	05.05.1998
Туркменистан	438	01	BCTI	+993 66	23.04.2001
Турция	286	02	Telsim	+90 542	19.12.1994
Турция	286	01	Turkcell	+90 532	01.08.1994
Турция			IS-TIM (Telek. Hizmetten AS)		30.05.2001
Уганда	641	01	CelTel	+256 75	01.04.1999
Уганда	641	10	MTN Uganda Limited	+256 77	18.06.1999
Узбекистан	434	05	Coscom	+998 93	21.07.1999
Украина	255	03	Kyivstar GSM	+380 67	02.04.1998
Украина	255	01	UMC Ukrainian Mobile Comm	+380 50	01.09.1997
Украина	255	02	Ukrainian Systems Ukraine	+380 68	29.03.1999
Фарерские острова	288	01	Faroese Telecom	+298 24	04.06.1999
Фиджи	542	01	Vodafone Fiji Ltd	+679	23.05.1997
Филиппины	515	01	ISLACOM	+63 915	17.07.1997
Филиппины	515	02	Globe Telecom	+63 917	01.07.1996
Финляндия	244	05	Oy Radiolinja Ab	+358 50	01.01.1993
Финляндия	244	12	G2	+358 44	27.02.2001
Финляндия	244	14	Aland	+358 45	04.04.2001
Финляндия	244	91	Sonera	+358 40	16.03.2000
Франция	208	10	SFR	+33 689	26.03.1993

Таблица П2.1. Данные по роумингу GSM 900 по состоянию на 12.06.2001 (окончание)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Франция	208	01	France Telecom	+33 609	09.03.1993
Хорватия	219	01	HRT Croatia	+385 98	14.10.1996
Хорватия	219	10	VIPnet	+385 91	06.07.1999
Чешская республика	230	02	EUROTEL Praha	+420 602	02.09.1996
Чешская республика	230	01	RadioMobil Czechia	+420 603	02.12.1996
Швейцария	228	01	Swisscom Mobile	+41 79	
Швеция	240	07	Comviq	+46 707	01.01.1993
Швеция	240	08	NordicTel (Europolitan)	+46 708	01.01.1993
Швеция	240	01	Telia Mobitel	+46 705, 706	01.11.1992
Шри-Ланка	413	02	MTN Sri Lanka	+94 77	07.04.1997
Шри-Ланка	413	03	Celtel	+947 24	12.02.2001
Эстония	248	01	Estonian Mobile Telephone	+372 50	03.02.1995
Эстония	248	03	As Ritabell Estonia Q GSM	+372 55	22.09.1997
Эстония	248	02	Radiolinja Eesti	+372 565	02.10.1995
ЮАР	655	01	Vodacom	+27 82	01.07.1994
ЮАР	655	10	MTN.	+27 83	15.10.1994
Югославия	220	02	Montenegro Promonte	+381 69	30.01.1998
Югославия, Сербия	220	01	Mobtel	+381 63	27.08.1997
Югославия, Сербия	220	03	Telecom Srbija	+381 64	31.01.2001
Югославия	220	04	Monet	+381 67	10.01.2001

Таблица П2.2. Данные по роумингу GSM 1800 по состоянию на 12.06.2001

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Австрия	232	05	Connect ONE	+43 699	31.07.1998
Австрия	232	07	Telering	+43 650	18.07.2000
Бельгия	206	20	KPN Orange Belgium	+32 486	27.07.1999
Великобритания	234	30	Mercury ONE 2 ONE	+44 956/958	27.03.1997
Великобритания	234	33	ORANGE	+44 973	25.10.1996
Венгрия	216	70	Vodafone	+36 70	03.12.1999

Таблица П2.2. Данные по роумингу GSM 1800 по состоянию на 12.06 2001 (окончание)

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Германия	262	03	E-plus	+49 177	01.10.1995
Германия	262	02	VIAG Interkom	+49 179	23.08.1999
Гонконг	454	12	Peoples Phone	+852 920	13 10.1997
Гонконг	454	16	Sunday	+852 923	30.09.1997
Гонконг	454	10	New World Telephone	+852 921	14.05.1998
Греция	202	01	Cosmote	+30 97	11.05.1998
Дания	238	30	Mobilix	+45 26	26.01.1998
Дания	238	20	Telia AS Denmark	+45 28	22.06.1998
Испания	214	03	Retevision	+34 656	06.05 1999
Испания	214	07	Telefonica Moviles	+34 609	14.07.1995
Италия	222	98	Blue	+39 380	28.09 2000
Италия	222	10	Omnitel - Vodafone	+39 34	01 10.1995
Италия	222	01	Telecom Italia	+39 33, 35, 39)	01.01.1993
Италия	222	88	Wind	+39 320	01.03.1999
Кувейт	419	03	Wataniya Telecom	+965 6	10.01.00
Лихтенштейн	228	01	Swisscom	+41 79	
Малайзия	502	17	Time Wireless (Sapura)	+60 17	01.10.1995
Малайзия	502	16	Mutiara	+60 16	16.12.1996
Малайзия	502	13	TM Touch	+60 13	31.08 2000
Мальта	278	21	Mobisle	+356 79	26.01 2001
Нидерланды	204	16	Ben	+31 624	23.11.1999
Нидерланды	204	12	Telfort	+31 626	09 11 1998
Нидерланды	204	20	DutchTone	+31 628	22 01.1999
Польша	260	03	Centertel	+48 501	13.05.1998
Португалия	268	03	Optimus	+351 933	20 08 1998
Россия, Москва	250	99	КБ «Импульс» (KB Impuls)	+7 095 доб 9017	01 10.1997
Румыния	226	03	CosmoRom	+40 96	05 07 2000
Сингапур	525	02	Singapore Mobilink	+65	01.10 1997
Сингапур	525	05	StarHub Pte Ltd	+65 98	08.05 2001
Таиланд	520	18	TAC	+66 16	15 10.1996
Тайвань	466	97	Taiwan Cellular Corp	+886 93	19.02.1998
Тайвань	466	88	KG Telecom	+886 9383	01.04.1998
Тайвань	466	01	Far EasTone Telecoms	+886 936	13.05.1998
Танзания	640	04	Vodacom Ltd	+255 744	28 05.2001
Украина	255	05	Golden Telecom Bancomsv	+380 44	07 11 1997
Филиппины	515	03	Smart	+63 918/919	28.04.1999
Финляндия	244	91	Sonera	+358 40	16 03.2000
Франция	208	20	Bouygues Telecom	+33 660	03.07.1997
Чешская республика	230	03	Cesky Mobil	+420 608	19.04.2000
Швейцария	228	01	Swisscom Mobile	+41 79	

Таблица П2.3. Данные по роумингу GSM 1900 по состоянию на 22.05.2001

Страна	Код страны MCC	Код мобильной сети MCN	Оператор	Международный код набора	Дата открытия роуминга
Канада	302	01	Microcell Canada	+1 514	23.09.1997
США	310	270	Powertel	+1-334 33	30.07.1999
США	310	310	Voicestream Midwest	+1 813	25.06.1999
США	310	200-260	Voicestream Wireless	+1 179...	01.10.1998
США	310	170	Pacific Bell Mobile	+1 209...	03 02.1998
США	310	150	Bell South Mobility	+1 423, 704, 803, 919	19.12.1997
США	310	160	Voicestream Eastcoast	+1 201	22.01.1997
Чили	730	01	Entel	+56 980-82	11.10.1999

Таблица П2.4. Данные по международному роумингу NATEL International

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Европа						
Австрия	Mobilkom Austria	15.02.94	A 1	A1	232	01
Австрия	max. mobil Telekommunikation GmbH	14.10.96	A max.	max.	232	03
Австрия (GSM1800)	Connect Austria	31.07.98	A CONNECT	CONNECT	232	05
Албания	Albanian Mobile Communications sh.a.	29.04.98	AL AMC	AMC	276	01
Андорра	STA	10.07.95	STA-MOBILAND	M-AND	213	03
Бельгия	Belgacom Mobile	01.07.94	B PROXIMUS	PROXI	206	01
Бельгия	Mobistar	14.10.96	B MOBISTAR	MOBI	206	10
Бельгия	KPN Orange Belgium NV	27.07.99	B ORANGE	ORANGE	206	20
Болгария	MobilTEL AD	12.02.96	BG MTEL GSM	MTEL	284	01
Босния и Герцеговина	PTT BIH	28.01.98	PTT-GSM BIH	BHGSM	218	90
Ватикан	Telecom Italia и Omnitel					
Великобритания	Cellnet	11.07.94	UK CELLNET	CLNET	234	10
Великобритания	Vodafone Ltd.	02.08.93	UK VODAFONE	VODA	234	15
Великобритания (GSM1800)	Mercury One-2-One	27.03.97	UK ONE 2 ONE	ONE2ONE	234	30

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Великобритания (GSM1800)	Orange PCS Ltd.	25.10.96	UK ORANGE	ORANGE	234	33
Великобритания, остров Джерси (графство)	Jersey Telecom	31.12.94	UK JERSEY TELECOMS	GT-GSM	234	50
Великобритания, остров Мэн (графство)	Manx Telecom	15.07.96	MANX PRONTO GSM	MANX	234	58
Венгрия	Pannon GSM	11.07 94	H PANNON GSM	PANNON	216	01
Венгрия	Westel 900 GSM	18.04.94	H WESTEL 900	W-900	216	30
Германия	DeTeMobil	01.01.93	D1-TELECOM	D1	262	01
Германия	Manesmann Mobilfunk GmbH	15.12.92	D2 PRIVAT	D2	262	02
Германия	E-plus	01.10.95	D E-PLUS	E-PLUS	262	03
Гернси	Guernsey Telecom	02.05.96	UK GUERNSEY TEL	GSY-TEL	234	55
Гибралтар	Gibtel	01.06 95	GIBTEL GSM	GIBTEL	266	01
Греция	Panafon	14.02.94	GR PANAFON	PAN	202	05
Греция	STET Hellas	13.06.94	GR TELESTET	TLSTET	202	10
Греция (GSM1800)	Cellular Operating System Mobile Tel.	11.05.98	GR COSMOTE	C-OTE	202	01
Дания	Dansk Mobil Telefon	18.11 92	DK SONOFON	SONO	238	02
Дания	TeleDenmark Mobil	01.11.92	DK TDK-MOBIL	TD MOB	238	01
Дания (GSM1800)	Mobilix	26.01 98	DK MOBLIX	MBIX	238	30
Дания (GSM1800)	Telia A/S, Denmark	22.06.98	DK TELIA	TELIA	238	20
Израиль	Parther Communications Company Ltd	17.12.98	IL ORANGE	ORANGE	425	01
Ирландия	Telecom Eireann	01.02.94	IRL EIR GSM	E-GSM	272	01
Ирландия	Esat Digifone	03.03.97	IR DIGOFONE	DIGI	272	02
Исландия	Iceland Telecom	01.02.95	IS SIMINN	SIMINN	274	01
Исландия	TAL Ltd.	22.07.98	IS TAL	TAL	274	02
Испания	Telefonica Moviles	14.07.95	E MOVISTAR	MSTAR	214	07
Испания	Airtel Movil S.A.	02.10.95	E AIRTEL	AIRTEL	214	01
Испания (GSM1800)	Retevision Movil S.A.	06.05.99	E AMENA	AMENA	214	03
Италия	Omnitel Pronto Italia	01.10 95	I OMNITEL	OMNI	222	10

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Италия (GSM1800)	Wind Telecomunicazioni SpA	01.03 99	I WIND	WIND	222	88
Кипр	Cyprus Telecom Authority	07.08.95	CY CYTA GSM	CY-GSM	280	01
Латвия	Latvian Mobile Telephone Co. Ltd.	10 04.95	LV LMT GSM	LMT	247	01
Латвия	Baltcom GSM	29.10.97	LV BALTCOM	B-COM	247	02
Литва	UAB Bite GSM, Vilnius	25.04.96	LT BITE GSM	BITE	246	02
Литва	Omnitel Lithuania	01.08.96	LT OMNITEL	OMT	246	01
Лихтенштейн	Swisscom Mobile		CH SWISS GSM	SWISS	228	01
Люксембург	P&T Luxembourg	01.07.93	L LUXGSM	LUXGSM	270	01
Люксембург (900/1800)	Milicom SA	18.09.98	L TANGO	TANGO	270	77
Македония	Post and Telecom Makedonija	01.07.97	MKD-MOBIMAK	MOBI-M	294	01
Мальта	Vodafone Malta Limited	19.08.97	M VODAFONE	VODA M	278	01
Молдова	VoxTel SA	22.02.99	MD VOXTEL	VOXTEL	259	01
Монако	France Telecom или SFR					
Нидерланды	Libertel BV	01.02.96	NL LIBERTEL	LIBTEL	204	04
Нидерланды	KPN Telecom BV	01.07.94	NL KPN TELECOM	NL KPN	204	08
Нидерланды (GSM1800)	Telfort Holding B.V.	09.11.98	NL TELFORT	TELFRT	204	12
Нидерланды (GSM1800)	Dutchtone NV	22.01.99	NL DUTCHTONE		204	20
Норвегия	Telenor Mobil AS	01.11.92	N TELENOR	TELENO	242	01
Норвегия	Netcom GSM AS	01 10.93	N NETCOM GSM	NCOM	242	02
Польша	Polkomtel S.A., Warsaw	04 11.96	PL PLUS	PLUS	260	01
Польша	Polska Telefonia Cyfrowa – PTC	06.12.96	PL ERA GSM	ERAGSM	260	02
Польша (GSM1800)	PTK Centertel	13.05.98	PL IDEA	IDEA	260	03
Португалия	Telecel	29.07.93	P TELECEL	TLCL	268	01
Португалия	Telecomunicacoes Moves Nac.	01.07.93	P TMN	TMN	268	06
Португалия (GSM1800)	Main Road Telecomunicacoes S.A.	20.08.98	P OPTIMUS	OPTIM	268	03
Россия (Москва)	Мобильные ТелеСистемы	01.02.96	RUS MTS	MTS	250	01

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Россия (Санкт-Петербург)	Северо-Западный GSM (North-West GSM, St.Petersburg)	15.03.96	RUS NORTH-WEST GSM	NWGSM	250	02
Россия (Екатеринбург)	Уралтел (Uraltel, Yekaterinburg)	10.07.98	RUS URALTEL	UTL	250	39
Россия (Краснодар)	Кубань GSM (Kuban-GSM, Krasnodar)	01.10.98	RUS KUBAN-GSM	KUGSM	250	13
Россия (Новосибирск)	Сибирские сотовые системы (Siberian Cellular Systems, Novosibirsk)	26.04.99	RUS SCS	SCS	250	05
Россия (Ростов)	Донтелеком (JSC Dontelecom, Rostov-on-Don)	12.10.98	RUS DONTELECOM	250 10	250	10
Россия (Самара)	СМАРТС (ZAO SMARTS, Samara)	02.03.99	RUS SMARTS	SMARTS	250	07
Россия (Ставрополь)	Телесот-Ставрополь (StavTeleSot, Stavropol)	01.06.99	RUS NORTH	NC-GSM	250	44
Россия, Москва (GSM1800)	КБ «Импульс» (KB Impuls, Moscow)	01.10.97	RUS KB IMPULS	KB IMPULS	250	99
Румыния	MobilRom	30.06.97	RO DIALOG	DIALOG	226	10
Румыния	MobiFon SA	12.08.97	RO CONNEX	CONNEX	226	01
Сан-Марино	Telecom Italia и Omnitel					
Словакия	Globtel (SK)	14.04.97	SVK GT	SVK GT	231	01
Словакия	EuroTel Bratislava	14.04.97	SK EUROTEL	ET-SK	231	02
Словения	MobiTel d.d., Slovenia	14.10.96	SI MOBITEL GSM	SI GSM	293	41
Словения	SI.MOBIL D.D.	26.04.99	SI MOBIL	SI. MOBIL	293	40
Турция	Telsim	19.12.94	TR TELSIM	TLSIM	286	02
Турция	Turkcell	01.08.94	TR TURKCELL	TCELL	286	01
Украина	Kyivstar GSM JSC	02.04.98	UA KYIVSTAR	UA-KS	255	03
Украина	Ukrainian Mobile Communications	01.09.97	UA UMC	UMC	255	01
Украина	Ukrainian Radio	29.03.99	UA FLASH	FLASH	255	02

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Фарерские острова	Faroese Telecom	04.06.99			298	24
Финляндия	Sonera Corporation	01.11.92	FI SONERA	SONERA	244	91
Финляндия	Oy Radiolinja Ab	01.01.93	FI RADIOLINJA	RL	244	05
Франция	Sosiete Francaise du Radiotelephone	26.03.93	F SFR	SFR	208	10
Франция	France Telecom Mobiles	09.03.93	F ITINERIS	Itine	208	01
Франция (GSM1800)	Bouygues Telecom	03.07.97	F BOUYGUES TELECOM	BYTEL	208	20
Хорватия	Croatian Telecom	14.10.96	HR CRONET	CRON	219	01
Чешская республика	EuroTel Praha	02.09.96	CZ EUROTEL	ET-CZ	230	02
Чешская республика	Radiomobil, Praha	02.12.96	CZ PAEGAS	PAEGAS	230	01
Швеция	Comviq GSM AB	01.01.93	S COMVIQ	IQ	240	07
Швеция	AB	01.01.93	S EUROPOLITAN	EURO	240	08
Швеция	Telia Mobite AB	01.11.92	S TELIA	TELIA	240	01
Эстония	EESTI Mobiltelefone	03.02.95	EE EMT GSM	EMT	248	01
Эстония	AS Ritabell	22.09.97	EE Q GSM	Q GSM	248	03
Эстония	Radiolinja Eesti AS	02.10.95	EE RLE	EE RL	248	02
Югославия, Сербия	Mobile Telecommunications "Srbija"	27.08.97	YU MOBTEL	MOBTEL	220	01
Югославия, Черногория	Promonte	30.01.98	YU PROMONTE	PMONTE	220	02
Арабские государства						
Бахрейн	Batelco	15.07.96	BHR MOBILE PLUS	M PLUS	426	01
Иордания	Jordan Mobile Telephone	08.08.97	JOR-FASTLINK	FSTLINK	416	01
Катар	Qatar Telecommunications Corp.	01.06.95	QAT-QATARNET	Q-NET	427	01
Кувейт	Mobile Telecom. Co. (K.S.C.)	01.08.95	KT MTC NET	MTC	419	02
Ливан	FTML	23.09.96	RL CELLIS	CLLIS	415	01
Ливан	LibanCell	12.09.96	RL LIBANCELL	LIBCL	415	03
Объединенные Арабские Эмираты	Etisalat	11.11.94	UAE ETISALAT	ETSLT	424	02
Оман (Султанат)	GTO Ministry of PTT	29.09.97	OMAN MOBILE	OMAN	422	02
Саудовская Аравия	Saudi Telecom Company	30.06.97	KSA ALJAWWAL	ALJAWWAL	420	01

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Саудовская Аравия	Electronic Application Establishment	11.01.99	KSA EAE	EAE	420	07
Африка						
Египет	ECMS MoBiNil	15.10.98	EGY MOBINIL	MOBINI	602	01
Египет	MisrFone Telecommunications Co., SAE	30.11.98	EGY CLICK GSM	CLICK	602	02
Зимбабве	Posts and Telecommunications Corp.	07.12.98	ZW NET*ONE	NET*1	648	01
Зимбабве	Econet Wireless	01.04.99	ZW 04	ZW 04	648	04
Кот-д'Ивуар	Societe Ivoirienne des Mobiles (SIM)	18.05.98	CI IVOIRUS	IVOIR	612	03
Кот-д'Ивуар	Loteny Telecom	09.03.98	CI TELECEL	TELCEL	612	05
Маврикий	Cellplus Mobile Telecom. Ltd.	06.06.96	MRU CELLPLUS	CELL+	617	01
Марокко	Itissalat Al Maghrib SA	27.03.95	MOR IAM	IAM	604	01
Намибия	Mobile Telecommunications Ltd.	01.10.96	NAM MTC	MTC	649	01
Реюньон (остров)	Ste Reunionnaise du Radiotelephone	05.08.98	F SFR REUNION	SFR RU	647	10
Сейшельские острова	Cable & Wireless (Seychelles) Ltd.	09.09.98	SEZ CELLULAR	SEYCEL	633	01
Сейшельские острова	Telecom Seychelles Limited	27.07.99	SEZ AIRTEL	AIRTEL	633	10
Сенегал	Sonantel S.A.	23.02.98	SEN SONATEL	SONATEL	608	01
Танзания	TRI Telecommunications (T) Ltd.	06.02.98	TZ TRITEL	TRITEL	640	01
Тунис	Tunisie Telecom, Tunicell	05.05.98	TUN TUNICELL	605-02	605	02
Уганда	CelTel Cellular	01.04.99	UG CELTEL	CELTEL	641	01
Уганда	MTN Uganda Ltd.	18.06.99	UG MTN	MTN-UG	641	10
ЮАР	Vodacom Pty Ltd.	01.07.94	SA VODACOM	VODA	655	01
ЮАР	Mobile Telephone Network Ltd.	15.10.94	SA MTN	MTN	655	10
Индия						
Индия (Бангалор)	J.T.Mobiles Limited	01.07.99	INA JT MOBILES	JT	404	45
Индия (Гуджарат)	Facsel Limited	15.03.99	INA FASCEL	FASCEL	404	05
Индия (Дели)	Bharthi Cellular Ltd.	28.09.98	INA AIRTL	AIRTL	404	10

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Индия (Дели)	Sterling Cellular Ltd.	26.08.98	INA ESSAR CELLPHONE	ESSAR	404	11
Индия (Калькутта)	Usha Martin Telecom Ltd.	09.12 98	INA COMMAND	COMMAND	404	30
Индия (Мадрас)	RPG Cellular Services Ltd.	25.06.99	INA RPG	RPG	404	41
Индия (Мадрас)	Skycell Communications Ltd.	26.03.99	INA SKYCELL	SKYCELL	404	40
Индия (Мамбаи)	Hutchison Max Telecom Pvt	15.12.98	INA MAXTCH	MAXTCH	404	20
Индия (Мамбаи)	BPL Mobile Communications Ltd.	07.03.99	INA BPL MOBILE	BPL MOBILE	404	21
Восточная и центральная Азия						
Азербайджан	Azercell Telecom	24.02.97	AZE AZERCELL GSM	ACELL	400	01
Азербайджан	J.V.Bakcell	09.06.99	AZE BAKCELL GSM	BKCELL	400	02
Грузия	Magticom Ltd.	19.02.98	GEO MAGTI-GSM	MAGTI	282	02
Грузия	Geocell Ltd.	08.09.97	GEO GEOCELL	GCELL	282	01
Казахстан	KaR-Tel LLC	23.06.99	KZ K-MOBILE	K-MOBILE	401	01
Кыргызстан	Bitel Ltd.	10.05 99	KGZ BITEL	BITEL	437	01
Пакистан	Pakistan Mobile Communications Ltd.	16.11.98	PAK MOBILINK GSM	MOBILINK	410	01
Узбекистан	Coscom	21.07.99	UZB COSCOM GSM	COSCOM	434	05
Азия, Тихоокеанский регион						
Австралия	Vodafone Pty Ltd.	15.07.94	VODAFONE AUS	VFONE	505	03
Австралия	Cable & Wireless Optus Ltd.	23.09.94	AUS YES OPTUS	OPTUS	505	02
Австралия	Telecom Australia (Telstra)	15.07.94	AUS MOBILENET	M-NET	505	01
Бруней	DST Communications	22.09.97	BRU DSTCOM	DSTCOM	528	11
Гонконг	SmarTone Mobile Comms	20.06.94	HK SMARTONE	HK SMC	454	06
Гонконг	Hutchison Telephone Co.	30.04.96	HK HTCLGSM	HTCL	454	04
Гонконг	HK Telecom CSL	16.01.95	HK TELECOM	TELCO	454	00
Гонконг	Peoples Telephone	13 10.97	HK PEOPLES	PTC	454	12

Таблица П2.4. Данные по международному роумингу NATEL International (продолжение)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Гонконг (GSM1800)	Mandarin Communications Ltd.	30.09.97	HK SUNDAY	SUNDAY	454	16
Гонконг (GSM1800)	New World PCS, Ltd.	14.05.98	HK NWT	NWT	454	10
Индонезия	PT Satelit Palapa Indonesia (Satelindo)	12.03.96	IND SATELINDOCEL	SAT-C	510	01
Индонезия	PT Telekomunikasi Palapa, Indonesia	02 09.96	IND TELKOMSEL	T-SEL	510	10
Индонезия	PT Excelcomindo Pratama	18 03.97	IND GSM-XL	EXCEL	510	11
Камбоджа	CamGSM Company Ltd.	14.12.98	KHM MOBITEL	MBTL	456	01
Китай	MPT, Chine Telecom	21.04.97	CHINA TELECOM	CT-GSM	460	00
Китай	Chine Unicom	25.06 99	CHN CUGSM	CU-GSM	460	01
Макао	C.T.M. Macau	15.03.96	MAC-CTM GSM	CTMGSM	455	01
Малайзия	Cellular Communications Network	07.10.96	MY-CELCOM GSM	CELCOM	502	19
Малайзия	Binariang Telecommunication Sdn Bhd	20.05 96	MY-MAXIS MOBILE	MAXIS	502	12
Малайзия (GSM1800)	Time Wireless (бывшая Sapura Digital)	01.10 95	MY ADAM 017	ADAM	502	17
Малайзия (GSM1800)	DiGi Telecommunications Sdn Bhd	16.12.96	MY DIGI 1800	DIGI	502	16
Новая Зеландия	Vodafone New Zealand	15.10 96	NZ VODAFONE	VODA	530	01
Сингапур	MobileOne (Asia) Pte Ltd, Singapore	24.03 97	SGP M1-GSM	M1-GSM	525	03
Сингапур	Singapore Telecom Mobile	15.10.94	SGP ST GSM	ST GSM	525	01
Сингапур (GSM1800)	Singapore Telecom Mobile	01.09.97	SGP ST GSM1800	GSM 1800	525	02
Таиланд	Advanced Info. Service PCL	15.09.95	TH AIS GSM	TH AIS	520	01
Таиланд	Total Access Communication PCL	15.10.96	TH TAC	TH TAC	520	18
Тайвань	TransAsia Telecommunications	26.05.98	TWN TRANSASIA	466 99	466	99

Таблица П2.4. Данные по международному роумингу NATEL International (окончание)

Страна	Оператор	Дата открытия роуминга	Наименование национальной сети	Код на дисплее	Код страны MCC	Код мобильной сети MCN
Тайвань	Chunghwa Telecom (LTDA)	01.02.96	TWN LDTA GSM	LDGSM	466	92
Тайвань (GSM1800)	Pacific Cellular Corp.	19.02.98	TWN GSM 1800	PCC	466	97
Тайвань (GSM1800)	KG Telecom Co.	01.01.98	TWN KGT ONLINE	KGT	466	88
Тайвань (GSM1800)	Far Eas Tone Telecommunications	13.05.98	TWN FAR EAS TONE	FET	466	01
Тайвань (GSM900/1800)	Tuntex Telecommunications Co Ltd.	01.07.98	TWN TUNTEX GSM	TUNTEX	466	06
Фиджи	Vodafone Fiji Ltd.	23.05.97	FIJ VODAFONE	VODA FIJ	542	01
Филиппины	Isla Communications Co., Inc.	17.07.97	PH ISLACOM	ISLA	515	01
Филиппины	Globe Telecom GMCR Jnc.	01.07.96	PH GLOBE TELECOM	GLOBE	515	02
Филиппины (GSM1800)	Smart Communications Inc.	01.06.99	PH SMART	SMART	515	03
Шри-Ланка	MTN Networks (PVT)	07.04.97	SRI DIALOG	DIALOG	413	02
Северная Америка (GSM 1900)						
Канада	Microcell Telecommunications Inc.	23.09 97	CAN MCELL	MCELL	302	01
США	Powertel PCS Partners	30.07.99	USA POWERTEL, INC	USA27	310	270
США	Aerial Communications, Inc.	25.06.99	USA AERAL	AERAL	310	310
США	Western Wireless Corp.	01.10.98	USA VOICESTREAM	WWC	310	210-260
США	Pacific Bell Mobile Services (California)	03.02.98	USA PBMS	PBMS	310	170
США	Bell South Mobility (Carolina's, TN)	19.12.97	USA BELL SOUTH MOBILITY	BSMDSC	310	150
США	Omnipoint (New York, Boston, Miami)	22.01.97	USA OMNIPOINT	OMNI	310	160
США	APC (Washington/ Baltimore)	07.11.97	USA SPRINT SPECTRUM	SPRINT	310	020
Спутниковая система (GPS)						
Весь мир	Iridium LLC	25.09.98			901	03

6.3. ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

Для успешной работы с программами, описанными в книге и размещенными на компакт-диске, необходимо, чтобы конфигурация вашего компьютера соответствовала требованиям, приведенным в табл. П3.1.

Таблица П3.1. Конфигурация компьютера

Конфигурация	Минимальная	Рекомендуемая
Процессор Скорость	486 DX4 100 МГц	Pentium > 166 МГц
RAM/жесткий диск	16 Мб/1,2 Гб	32 Мб/>1,2 Гб
Система	Windows 95	Windows 98
Видеоплата/монитор	VGA/14"	SVGA/15"
Устройство для чтения дискет	HD	HD
Устройство для чтения компакт-дисков	2x	>12x
Периферийные устройства • Звуковая плата • Принтер • Устройство для считывания чип-карт • Программатор компонентов	 – Матричный Изготовить собственными силами –	 8/16 бит Струйный или лазерный PS/SC PIC 16C/F 84
Установленное программное обеспечение	Acrobat Reader (прилагается)	Acrobat Reader (прилагается) Доступ к Internet Комплект BasicCard (прилагается)

6.4. БИБЛИОГРАФИЯ

1. Гелль П. Чип-карты. Устройство и применение в практических конструкциях. М.: ДМК, 2000.
2. Гелль П. ПК и чип-карты. М.: ДМК, 2001.
3. Donio J., Leroux les Jardins J., de Rocca E., Verstrepen M., La carte a puce, Paris, Presses Universitaires de France, «Que sais – je?» 1999.

Патрик Гёлль

Мобильные телефоны и ПК

Главный [illegible] *Захаров И. М.*
[illegible]press.ru
Перевод *Брод Т. Е.*
Выпускающий редактор *Морозова Н. В.*
Верстка *Дудатий А. М.*
Графика *Салимонов Р. В.*
Дизайн обложки *Дудатий А. М.*

Подписано в печать 16.02.2004. Формат 60×88 1/16.
Гарнитура «Петербург». Печать офсетная.
Усл. печ. л. 14,21. Тираж 1000 экз. Зак. № 247

Издательство «ДМК Пресс», 105023, Москва, пл. Журавлева, д. 2/8.
Web-сайт издательства: www.dmk.ru
Internet-магазин: www.dmk.ru, www.abook.ru

Отпечатано в типографии № 9. Волочаевская, 40.