

Сергей Жуков

# Хакинг мобильных телефонов

УДК 004.5  
ББК 32.973.26-018.2  
Ж55

**Жуков С.**

Ж55 Хакинг мобильных телефонов / Сергей Жуков. - М.: Бук-пресс, 2006. - 224 с. - (Серия книг «Tips and Tricks»).

ISBN 5-85493-096-3

Описание секретов и методов взлома сотовых средств связи.

УДК 004.5  
ББК 32.973.26-018.2

ISBN 5-85493-096-3

© Карабин П., составление, 2006  
© Бук-пресс, 2006

# Содержание

## Мобильная, сотовая и спутниковая связь

Стандарты и операторы .....	5
Виды телефонов и переадресация .....	20
Роуминг .....	62
Радиотелефоны .....	66
Радиосредства .....	72
Индукционные передатчики и приемники .....	80
Globalstar .....	82
Ретрансляторы .....	101

## Взлом

Мобильная связь .....	105
GSM .....	109
SIM карточки .....	109
FraudBuster .....	112
Ловушки .....	115
Клонирование .....	123
Выявление местоположения абонента .....	125
Шифрование .....	131
Пейджеры .....	135

## **Содержание**

---

Секретные коды .....	139
Двойники .....	148
AKEY .....	149
SIS .....	152
Недокументированные возможности .....	153
Прослушивание .....	158
Дело было еще в конце 1993 года... ..	158
Фрод .....	181
Трюки с пейджером .....	191
GSM-безопасность .....	195

## **Приложения**

Толковый словарь .....	198
Использованные материалы .....	216

## Мобильная, сотовая и спутниковая связь

Мобильная связь — это любая радиосвязь, позволяющая абоненту пользоваться ею без привязки к конкретному месту: сотовая, транковая (или транкинговая), пейджинговая, радиотелефоны, радиоудлинители,рации.

Сотовая связь — разновидность мобильной связи, организованная по принципу сот или ячеек (cells), путем размещения базовых станций (БС) (Base Transceiver Station), которые покрывают локальную территорию. Совокупность локальных территорий составляет зону обслуживания (ЗО) оператора. Уровень сигнала в конкретном месте зависит от близости к БС, рельефа местности, застройки, промышленных помех и других факторов. Сигнал с БС передается на коммутатор и обрабатывается им.

Карты ЗО операторы публикуют, к примеру, на своих сайтах. У Московских операторов карты не очень наглядные — во-первых, они публикуют их без указания ме-

стоположения БС (неуклюже ссылаясь на секретность и мифические приказы Мин-Связи), что снижает их информативность, во-вторых, иногда показаны всего 3 градации уровня сигнала: отсутствие сигнала, зона возможного приема и зона уверенного приема.

Причем, вместо логичной для наглядности цветовой гаммы — белый, светлый, темный соответственно — у Билайна, к примеру, на картах так — белый, темный, светлый. Может, для обмана зрения? Взглянешь на карту — все темное, а на самом деле — это зона всего лишь возможной связи. К тому же эти карты часто представляют желаемое за действительное — отмечено, что есть связь там, где ее нет. По карте Билайн-GSM радиоэфир покрывает территорию ровным слоем, совершенно не видно рельефа.

На карте МТС зона покрытия размечена более детально, можно в большой доле вероятности определить наличие связи даже в разных концах одной деревни, тем более что у нее более крупный масштаб. МСС зачем-то рисует на своей карте на сайте зоны обслуживания операторов из соседних регионов, но ведь зона обслужива-

ния МСС ограничивается границей Московской области. Это вводит в заблуждение абонентов-новичков. Хотя МСС и делает ремарку, что «МСС несет ответственность за услуги связи, предоставляемые в границах Московской области», но это можно понять и так, что за границей Московской области МСС услуги связи предоставляет, только не несет за них ответственности. Такая же сомнительная карта висит и в офисах МСС.

Многие региональные операторы секторов Полишинеля не практикуют. Например, образцовая карта у С.-Петербургского оператора Fora — и БС указаны (даже публикуются список точных адресов их установки), и 7 градаций сигнала.

### Стандарты и операторы

Стандарт сотовой связи — это система технических параметров и соглашений для обеспечения функционирования системы сотовой связи. В России приняты 4 стандарта сотовой связи. О них уже много написано, к примеру, в разделе Мобильная связь на iXBT, но хотелось бы акцентировать внимание на некоторых моментах.

NMT-450i (Nordic Mobile Telephone) — старый аналоговый стандарт. В Москве этот стандарт поддерживает МСС (Московская Сотовая Связь). Все российские NMT-Операторы образуют сеть СоТел (сотовый телефон России). Иногда можно услышать или прочитать мнение, что качество NMT-связи плохое.

Это не так.

Часто такое мнение навязывают дилеры, большинство из которых подключает только к Билайн и МТС из-за более выгодных своих комиссионных от оператора. МСС-дилеров гораздо меньше, да и менее выгодна МСС для дилеров. Качеству связи — это понятие комплексное: зона покрытия, чувствительность, легкость дозвона, проникаемость, качество звука, устойчивость соединения, поэтому качество связи надо рассматривать по отдельным параметрам. Все эти параметры у NMT-450i на уровне цифровых стандартов. Иногда ругают NMT-звук, но он не плохой, он просто другой: да, иногда есть характерные «хрюки», при неустойчивой связи есть шумы.

Но сам звук более естественный, «живой» и насыщенный по сравнению с цифровыми стандартами, нет цифрового «буль-

канья», «кваканья» и провалов. В случае, если в условиях плохой связи, в шумном помещении или на оживленной улице по NMT-телефону еще как-то можно понять собеседника, даже сквозь треск и шум, то в GSM (особенно московского разлива) зачастую понять нельзя ничего. Иногда в NMT-450i плохой прием внутри помещений в местах плотной застройки или «грязного» эфира (проницаемость в NMT-450 несколько хуже, чем в GSM). NMT-связь устойчивая, разрывает редко (гораздо реже, чем GSM), а в смысле площади покрытия стандарту NMT-450i вообще нет равных.

В случае, если нужна связь из удаленных мест, то это то, что надо, особенно с мощными телефонами. При определенных условиях, абонент может пользоваться NMT-телефоном на удалении до 100 км от БС, поэтому этот стандарт еще долго будет жить на необъятных просторах России, главное, чтобы МСС и СоТел его не забросили, да чиновники не мешали (пока все тихо).

К недостаткам стандарта NMT можно отнести «привязку» телефона к оператору, завышенные цены на телефоны вследствие уже небольших объемов выпуска, большой

размер телефонов, скудный их выбор. Спасибо Benefon'у — выпустил новую модель Exion длиной 100 мм и мощностью 1,2 Вт. Другую полезную информацию о стандарте NMT-450 и телефонах, ссылки и отзывы абонентов можно почитать на странице абонентов МСС.

D-AMPS (Digital Advanced Mobile Phone Service) — цифровой стандарт. В Москве его поддерживает Билайн-800 (Вымпелком, далее Билайн-DAMPS). Высокое качество связи, хороший звук (по сравнению с GSM), довольно популярен в России, так же, как и его аналоговый вариант AMPS и его разновидности xAMPS. К сожалению, Билайн, похоже, заморозил развитие сети DAMPS, видимо под впечатлением чиновничьего ограничения лицензий на DAMPS-связь 2010-м годом. Посмотрите на карту Билайн-DAMPS, если убрать темный цвет (а это всего лишь зона возможной связи), то что останется? А ведь, учитывая высокое качество сети DAMPS, ее можно было хорошо раскрутить. ( -примечание: здесь и далее подразумевается Билайн как торговая марка московской компании Вымпелком).

GSM (Global System for Mobile communications) — современный цифровой стандарт (основной во многих странах).

Большое преимущество стандарта — он «непривязанный» — телефонный номер и вся другая информация об абоненте записана в SIM-карте (Subscriber Identity Module), которая выдается абоненту при заключении контракта и может вставляться в любой (нелоченый) аппарат GSM нужного диапазона, что делает независимым (в этом смысле) сам аппарат от оператора.

Каждый сотовый GSM-аппарат имеет собственный уникальный номер — IMEI (International Mobile Equipment Identity — международный идентификатор мобильного устройства), по которому контролируется работа аппарата в GSM-сети. IMEI «прошивается» в GSM-телефон при его производстве и для его смены нужно специальное дорогостоящее оборудование. IMEI GSM-телефона можно посмотреть на наклейке под аккумулятором телефона или в самом телефоне, набрав на телефоне #06#. Кстати, при покупке GSM-телефона проверяйте, чтобы эти номера совпадали. Стандарт GSM подразделяется на GSM-450/900/1800/1900 в зависимости от рабочей

частоты. Кстати, почему-то GSM-450 официально называют GSM-400 — кстати, его развитие под большим вопросом. Максимальное удаление абонента от БС в GSM-900 около 35 км, в GSM-1800 около 6 км, поэтому сеть GSM-1800 должна быть гораздо плотнее, а следовательно она требует гораздо больших капиталовложений. В Москве стандарт GSM поддерживают МТС (Мобильные ТелеСистемы) и Билайн-GSM (Вымпелком). У МТС основная сеть GSM-900 плюс базовые станции GSM-1800 в проблемных местах (большой нагрузки) — центр Москвы, Ленинградское шоссе и некоторые другие.

Как показывает практика, сеть МТС в последнее время частенько не справляется с нагрузкой. У Билайна-GSM первоначальная сеть GSM-1800, ею сейчас покрыты Москва и ближнее Подмосковье (по разным направлениям — 20-50 км от МКАД). Потом Билайн-GSM стал строить сеть GSM-900/1800, ею уже покрыт почти весь Московский регион. Кстати, в Билайне-GSM однодиапазонные телефоны GSM-900 работают уже почти также, как GSM-900/1800, хотя официально Билайн их не подключает.

Сеть МТС есть на некоторых станциях метро и работа по ее расширению постоянно ведется. Это важно для многих — во-первых, сотовая связь стала доступной для многих слоев населения, а, во-вторых, по Москве сейчас зачастую быстрее проехать на метро, чем торчать в автомобильных пробках, поэтому наличие сети в метро — для многих весомый аргумент в пользу МТС. Билайн-GSM тоже строит сеть в метро, но пока связь от Билайн-GSM есть только на станции Таганская.

В 2001 году в Московском регионе третий GSM-Оператор в Москве Соник Дуо планирует ввести в эксплуатацию свою сеть.

CDMA (Code Division Multiple Access) — современный цифровой стандарт, по многим техническим характеристикам превосходящий GSM. В Москве стандарт CDMA поддерживает Сонет (Персональные Коммуникации). В России стандарт CDMA почему-то сертифицирован только как «фиксированный», хотя все абоненты пользуются им, естественно, как мобильным. Будем надеяться, что CDMA в России преодолееет рогатки чиновников, зачастую ориентирующихся на личные интересы, и под-

стрекаемых другими ОпСоСами. В CDMA — хороший насыщенный звук, устойчивая связь.

Максимальное удаление абонента от БС связи определяется только мощностью передатчика и чувствительностью приемника. Практически на коммерческих сетях CDMA реализован радиус 140 км. Недостатки Сонета: пока еще более дорогие (чем в GSM) телефоны, небольшая зона покрытия (Москва и ближнее Подмосковье). У CDMA есть (а может уже был?) еще один серьезный недостаток — привязанность телефона к оператору (об этом смотри ниже), но, оказывается, это не фатально. Осенью 2000-го года китайская фирма ZTE под чутким руководством лидера CDMA-технологий фирмы Qualcomm выпустила первый в мире CDMA-телефон с SIM-картой.

Это маленькая незамеченная революция, возможно, положила начало превращению стандарта CDMA из «привязанного» в «отвязанный». В случае, если CDMA действительно избавится от «привязанности», то, учитывая технические преимущества этого стандарта, он станет еще более привлекательным. Хочется верить, что российские чиновники от связи, несмотря на дав-



ление других операторов, отменят свой приказ о назначении этого стандарта «фиксированным» в России. Тем более, что, скорее всего, от CDMA-технологии все равно никуда не деться — похоже, именно эта технология будет использоваться в мире в сетях связи третьего поколения. Возможно, что и MCC будет строить свою CDMA-сеть.

Периодически разгораются споры о том, какой стандарт сотовой связи наименее вреден. На мой взгляд, это тема во многом надуманна, так же как и о вреде мобильных вообще — часто так называемые «исследования» на эту тему просто являются оплаченным заказом от заинтересованных организаций на получение нужного им вывода.

Иногда поднимается тема двойников в сотовой связи. Сегодня это уже практически невозможно у тех операторов, которые ввели специальные защитные меры (к примеру, все московские операторы), а раньше было весело — можно почитать воспоминания на эту тему Малициуса Фрода (здесь продолжение) или RadioGubitel'я.

Стандарты xAMPS, NMT-450i, CDMA являются «привязанными» стандартами. Во-первых, телефон «привязан» к опе-

ратору технически и административно, то есть оператором прошивается (программируется) сам телефон (а не SIM-карта, как в GSM), что является большим минусом для абонентов, доставляет им много неудобств, делает сам телефон (а, следовательно, и абонента) полностью зависимым от оператора. Во-вторых, абонентский номер (а также тариф) привязаны к телефону (аппарату). Это, а также небольшие по сравнению с телефонами GSM объемы производства, дает возможность завышения цен на телефоны, а также возможность введения различных сложностей — технических и административных.

Вот некоторые типичные ситуации и сравним их для «привязанных» стандартов и для GSM, нюансы зависят от конкретного оператора:

### Телефон сломался

Привязанный — везете телефон в сервис-центр, сдаете в ремонт со всеми вытекающими «геморроидальными» последствиями. То время, пока вы ждете возвращения вашего телефона к нормальной жизни, течение вашей жизни нарушается — ваш номер не функционирует. Мало, кто из операторов предоставляет на время ремонта дру-

гой телефон с тем же номером. А если телефон сломался где-нибудь вдали от ремонтной цивилизации, то совсем плохо. В случае, если телефон на гарантии, то вам могут выдать на время ремонта другой телефон с вашим же номером (по закону — через три дня после обращения, да и то не всегда), но для этого надо ехать только в определенные сервис-центры, для удаленных районов — «удобства» налицо. Кстати, пока телефон неисправен, то абонентская плата будет все равно тикать, или приближаться срок окончания действия карты, к примеру, БИ+ (то есть увеличиваться обязательная плата за трафик).

Можно, конечно, заблокировать телефон или даже написать заявление о продлении срока карты, но это дополнительные хлопоты, да и не всегда возможно. Некоторые операторы на время ремонта (или до покупки другого телефона) могут сделать на своем коммутаторе переадресацию на другой телефон (чтобы не пропадали звонки), но в порядке исключения. Иногда непонятно, что глючит — ваш аппарат, ваш номер телефона или сеть оператора. Определить это на привязанных стандартах затруднительно. Да и простая смена прошивки (требующая какого-то времени) или посажен-

ная батарейка (при отсутствии по рукой зарядного устройства) делает невозможным использование «привязанного» телефона.

GSM — переставляете SIM-карту из сломанного телефона в другой телефон GSM. В качестве временки в любом городе можно купить бэушный телефон старой модели долларов за 20 (или взять на время телефон у знакомых), и пользуетесь вашим номером, как раньше. Сломанный телефон можно, не торопясь, отдать в ремонт или продать как неисправный и купить новый. А кому-то... понравится временка за 20 долларов.

### **Вы решили сменить телефон (но сохранить свой номер)**

Привязанный — покупаете телефон. В случае, если бэушный, то могут быть сложности — можно нарваться на активный (еще не отключенный), тогда его не подключат. В случае, если не активный, то его сложно полностью проверить на работоспособность — к примеру, нельзя позвонить на него. Далее — едете в офис оператора, тратите время, пишете бумаги и ждете, когда вам «перекинут» номер (на бэушный или на новый). Можно поехать к оператору со старым владельцем бэушного телефона, но мало,

кто согласится на это тратить время. В новый аппарат надо заново «забивать» данные в записную книжку.

GSM — покупаете телефон (новый или б/у) и переставляете в него свою SIM-карту (на которой есть и ваша записная книжка).

**Вы решили подключиться с тем же телефоном к другому оператору (или временно воспользоваться его услугами)**

Привязанный — другой оператор может не подключить ваш телефон, пока телефон числится активным у другого оператора — NMT-телефон точно не подключат, в Co-Tel'е с этим особенно строго, в DAMPS'е или CDMA с этим проще. Процедура «отвязки» требует времени, у какого-то оператора немного, у какого-то (к примеру, у MCC) это довольно долго.

GSM — вставляете в свой телефон (нелоченый, конечно) SIM-карту другого GSM-Оператора и пользуетесь. Например, во время сбоя МТС или Билайн-GSM можно на всякий случай носить с собой SIMку другого оператора. Или в другом городе зачастую гораздо дешевле подключить к местному GSM-Оператору, чем пользоваться роумингом, тарифы на который за-

частую завышены и иногда случаются обсчеты абонентов в роуминге, с которыми трудно разобраться. Единственное неудобство — номер другой будет. Но, по крайней мере, местного оператора можно использовать для местной связи.

**Вы решили продать телефон**

Привязанный — конечно, можно просто продать телефон без смены владельца, не мудрствуя лукаво. Но есть вероятность, что ваш бывший телефон (точнее его номер) может влипнуть в какую-либо историю, а беспокоить будут вас, как юридического владельца телефона. Поэтому лучше продавать телефон официально через смену владельца или путем расторжения контракта и подключения телефона заново. Излишне говорить, что это связано с дополнительными хлопотами и материальными затратами.

GSM — вынимаете свою SIM-карту и продаете телефон. Можно таким же образом легко купить другой. К слову сказать, что повод поменять GSM-телефон всегда есть — новые модели появляются постоянно. Множество моделей, современные, с великолепным дизайном на любой вкус, технически навороченные, некоторые из них с

отличным качеством, в том числе звука, так и подбивают купить себе что-то новенькое. DAMPS- и NMT-абоненты лишены такого удовольствия — они вынуждены выбирать телефон из десятка устаревших моделей — производители телефонов уже практически не балуют эти стандарты (особенно NMT-450i) своим вниманием.

Самые большие сложности, связанные с привязкой телефона, в МСС (и вообще в NMT-450i) — без официальной отвязки от NMT-Оператора телефон не подключат нигде. «Хирургическое вмешательство» в NMT-телефон для переподключения доступно только специалистам и сейчас уже не всегда экономически целесообразно. В МСС еще существует практика неподключения так называемых «долговых» телефонов, то есть телефонов, за владельцами которых числится долг. Непонятно, причем здесь телефоны? Долг числится за абонентом, с него и надо требовать возврат долга, но почему-то «отыгрываются» на телефоне — без уплаты долга за предыдущего владельца телефон не подключат в МСС и не «отпустят». Слава богу, периодически МСС проводит «долговые амнистии», то есть акции по подключению к МСС долговых телефонов.

Так что недостатки «привязанных» стандартов налицо. Особенные строгости в России с NMT-450i, может быть, это связано с тем, что это федеральный стандарт, в отличие от DAMPS и CDMA. Повторюсь, радует начало выпуска CDMA-телефонов с SIM-картой, так что есть вероятность того, что CDMA перестанет быть «привязанным» стандартом и дело останется за «малым» — «отвязаться» от российских чиновников от связи.

## Виды телефонов и переадресация

### Прямые и кривые номера

Номера сотовых телефонов могут быть прямыми и кривыми. Прямые — это обычные городские семизначные (в Москве) номера, кривые (или федеральные) — набирать через коды 901, 902, 903, 501 или другие, с телефонов МГТС набираются через выход на межгород по «восьмерке» или через службу дозвона (СД) (или «альтернативный дозвон», или «звонок через коммутатор»).

### Преимущества прямого номера

- легкость дозвона, не надо пользоваться СД (не всегда есть возможность пользования тональным набором), «восьмеркой», которая все чаще бывает занята (когда же МГТС займется этим капитально?), а у кого-то «восьмерка» вообще заблокирована
- можно звонить с любых телефонов и таксофонов
- престижно, легко запомнить, нужно для бизнеса

**Важно:** Прямые номера, начинающиеся на «7» часто глючат — при наборе «7» с некоторых АТС иногда идет отбой, а иногда сразу после набора номера (до соединения с номером) идут короткие гудки — это заняты меж-АТС-ные каналы, а не сам номер. Это глюки МГТС, пора бы ей обратить на них внимание, ведь абоненты платят немалые деньги за прямой номер.

Абоненты МСС с прямым номером фактически имеют два номера — прямой и соответствующий ему кривой.

### Преимущества кривого номера

- ниже стоимость абонентской платы и времени эфира
- хорошо работает АОН

СД или Альтернативный дозвон — это бесплатная услуга операторов для звонков на кривые номера без набора «восьмерки» (не всегда есть возможность, да и иногда «восьмерка» бывает занята).

Для звонков по альтернативному дозвону телефон аппарат (обычный) надо перевести в тоновой режим (обычно это делается нажатием «звездочки»), а затем набрать номер мобильного телефона, в МСС надо просто попросить барышню набрать номер. Кстати, МСС давно обещала ввести и автоматическую службу дозвона, но пока «воз и ныне там». Так же БиЛайн никак не может сделать альтернативного дозвона по некоторым номерам по коду 903.

### Номера альтернативного набора

- МТС 766-02-22
- МСС 743-7777
- БиЛайн 743-0000, 795-5555, 747-9977,

961-9999, 974-9999 — несколько телефонов, предназначенные для разных сетей (Билайн-GSM или Билайн-DAMPS) и тарифов вносят путаницу. При наборе номера абонента надо заменить первую «7» номера на «0» (коммутатор об этом не предупреждает).

### ● Сонет 787-67-67

Можно воспользоваться альтернативным дозвонком и с некоторых таксофонов. Некоторые таксофоны переводятся в тоновый режим после нажатия кнопки подтверждения соединения (изображение трубки), некоторые — еще одним нажатием кнопки ответа (на больших синих таксофонах) или нажатием на «» (на более компактных таксофонах с металлической скошенной передней панелью). При звонках с других таксофонов, а также с обычных дисковых телефонов можно использовать биппер — генератор тоновых сигналов. МГТС обещает улучшить эту ситуацию — МК от 16.05.01: «Как сообщили МК в МГТС ...в ближайшие год-два в Москве будет решена проблема выхода на федеральные номера сотовых операторов. Благодаря этому москвичи смогут звонить... на мобильные теле-

фоны, номера которых начинаются с «восьмерки», с любого городского таксофона».

Звонки на кривые телефоны с телефонов МГТС считаются местными (для частных лиц бесплатны) только на серии московских операторов (независимо от того, где находится абонент). На кривые номера по кодам 901, 902, 903 других операторов звонки с телефонов МГТС платные. Для того, чтобы не попасть на деньги, можно посмотреть список телефонных серий.

### **АОН (Автоматический Определитель Номера)**

АОН — точнее в сотовой связи это называется CLIP (Calling Line Identification Presentation). При наличии такой услуги на дисплее мобильного телефона высвечивается номер звонящего Вам абонента. Кроме обычного своего назначения — знать, кто вам звонит, АОН полезен и в целях экономии. Например, в зависимости от определившегося номера, абонент может ответить или не отвечать, а переадресовать звонок, или ответить, уложившись в БП, или перезвонить с городского телефона. Или посмотреть позже список пропущенных звонков, если не было возможности ответить сразу. Или для того, чтобы отвечать только на вну-

трисетевые звонки, так как входящие мобильные звонки того же оператора бесплатны у многих операторов, к примеру, МТС и Билайн. В Билайн-GSM бесплатны (с некоторыми оговорками) звонки с Билайн, МТС и МСС. Но даже если АОН определил мобильный телефон, то нет гарантии, что такой входящий звонок будет для вас бесплатным — в Билайне принадлежность номера к какому-либо оператору определяются по данным коммутатора Билайна. Еще такой момент — может определиться номер абонента той же сети, но абонент, звонящий вам, находится в роуминге, а такие входящие звонки платны, так как они не относятся к внутрисетевым.

К сожалению АОН у ОпСоСов более-менее нормально работает только на кривых номерах. На прямых номерах определяются, в основном, только мобильные (и цифровые) телефоны. На прямых номерах АОН работает хорошо только у Сонета, а также на сериях 231, 233 у МТС, и 130, 136 у Билайн-GSM (тариф Супер-GSM). Вообще странно, что у операторов до сих пор нет полноценного АОНа. Понятно, что есть какие-то технические проблемы, в том числе у МГТС, но их давно пора решать, а не брать деньги за кастрированный АОН. И по-

чему на Сонете определяются почти все номера, причем на прямых номерах? У них что, звонки имеют особую маршрутизацию, минуя МГТС? Билайн до сих пор не может сделать корректное определение его номеров по коду 903 — часть номеров определяется как 901, что вносит путаницу и неудобства.

Принадлежность определившегося звонка можно посмотреть в списке телефонных серий.

АнтиАОН (CLIR) — позволяет скрыть свой номер от вызываемого абонента. операторы предоставляют услугу антиАОНа, который скрывает номер только от мобильных АОНов. Кстати, все телефоны МСС и некоторые телефоны Билайна не определяются на АОНах МГТС, то есть имеют как бы недокументированный антиАОН. У Сонета есть антиАОН и от мобильных, и от МГТС-ных АОНов, причем анти-АОН может быть как позвонковым — надо перед номером набирать «0» (плюс 0.12\$ к стоимости звонка) или постоянным за 6\$ в месяц.

### **Бесплатный порог — подачка вместо посекундки**

Бесплатный порог при исходящем/входящем звонке в секундах (БП исх/вх) — нетарифицируемый интервал, то есть отрезок времени от начала разговора, который не тарифицируется оператором, проще говоря — продолжительность разговора, за который не берется плата. Полезная штука — если кто-то позвонил вам по ошибке, или если вы кому-то звоните, а вместо абонента включается АОН, автоответчик (при их включении идет отсчет времени) или нужного человека нет дома, то при наличии БП не придется платить за несостоявшийся разговор за целую минуту (на большинстве ТП). Контроль БП в NMT-, DAMPS-, CDMA- телефонах затруднен при исходящем звонке, так как они показывают время не с начала разговора, а с момента соединения.

У МСС на большинстве ТП — 10исх/15вх (реально меньше), на тарифе МСС-Секунда бисх/6вх, на тарифе МСС-Супер-Минута — 1 минута. У Билайн-DAMPS БП — 9исх/9вх. У МТС и Билайн-GSM БП очень мал — 5исх/5вх. Трудно уложиться в это время даже одной фразой про «неправильный набор номера». А если

учесть возможную разницу в измерении времени аппаратурой оператора и аппарата абонента, то можно быть уверенным, что разговор абонента МТС не тарифицировался, только если на дисплее телефона 3 сек или меньше. Ведь, к примеру, если на вашем телефоне показано 4 сек, то это может быть 4.99 сек. А по данным аппаратуры МТС, предположим, 5.01сек (вполне реальная погрешность), то есть этот звонок про-тарифицируется.

### **БП не действует при переадресованных звонках.**

Проблему БП решило бы введение настоящей посекундной оплаты (то есть с первой минуты) или дискретно-посекундной. Настоящая посекундная оплата есть у МСС на тарифе Секунда, а у Сонета на всех повременных тарифах. У МТС и Билайн-GSM посекундная тарификация начинается только со второй минуты (что не всегда упоминается в рекламе). На большинстве ТП МСС, а также у всех ОпСоСов при междугородних и переадресованных звонках, действует поминутная тарификация с округлением (естественно для ОпСоСов) в большую сторону, причем округление лихое — 1 минуту 01 сек разговора зачтут за 2 ми-



нуты, то есть стоимость минуты получается в этих случаях дороже почти в 2 раза.

### Переадресация

Переадресация — автоматическое перенаправление звонка на другой телефон. Переадресация может быть безусловная (все звонки) или условная (если абонент занят, не отвечает или недоступен). В GSM возможно регулирование времени «неответа», после которого произойдет переадресация. В CDMA от Сонета регулирование этого интервала возможно пока только через Техническую Службу. Также в GSM возможно включение переадресации после поступления звонка — для этого надо нажать, к примеру, на отбой (естественно, заранее должна быть активирована переадресация «по занято» на какой-либо номер). К сожалению, нет возможности переадресовывать звонок после ответа. В Сонете безусловная переадресация зачем-то сопровождается голосовым сообщением звонящему абоненту о том, что его звонок переадресован. К сожалению, московские операторы пока не поддерживают услугу «Перевод звонка», то есть переадресация звонка после ответа.

Переадресация — полезная услуга для различных случаев:

- в целях экономии можно делать переадресацию на другой телефон, в том числе и МГТС.
- если телефон какого-либо оператора недоступен в конкретном месте (или неисправен), то можно переадресовывать звонок на доступный телефон. В случае, если телефон неисправен, то некоторые операторы могут сделать временную переадресацию на нужный вам номер (чтобы не терялись звонки), но в порядке исключения. Также через некоторых операторов можно отменить услугу переадресации, если нет возможности сделать это с телефона. В МТС это можно сделать даже через Internet (через ИС-СА).
- если необходим прямой номер, а, опять же, для экономии, можно переадресовывать звонки с него на телефоны с другими ТП.
- если требуется скрыть основной номер.

Для переадресованных звонков не действует бесплатный порог и округление поминутное в большую сторону.

У некоторых коммерческих «проводных» операторов есть услуга по предоставлению виртуального номера, переадресацией по различным алгоритмам, автоответчиком и другими сервисными функциями. Удобно при переходах к другому оператору — номер останется тот же. Можно воспользоваться услугами различных компаний по предоставлению номера, иметь постоянный «виртуальный» номер телефона и переадресовывать звонок на тот мобильный телефон, который в данный момент имеется у абонента.

При пользовании коммерческими проводными операторами дешевле звонить по межгороду, а также, используя переадресацию, иметь московский номер, постоянно находясь в другом городе. Правда, пока такие услуги дороговаты и интересны, в основном, организациям, но в некоторых случаях подойдут и частным лицам. Например, Ситек предоставляет услугу Виртуальный телефон — подключение 360\$ плюс 22\$ в месяц (включает обработку входящих звонков на 550 минут в месяц). У МТУ-Информ есть услуга Лоджик Лайн — подключение 120\$ плюс 99\$ в месяц (включает обработку 3300 минут в месяц), многоканальный номер.

Наиболее выгодные условия у Совинтел'а, который предоставляет услугу Персональный номер — один из вариантов: подключение 150\$ плюс 1,2\$ в день (примерно 36\$ в месяц), включает бесплатную переадресацию на московские и сотовые номера, в том числе кривые, без ограничения трафика. У всех этих компаний есть и различные дополнительные услуги при предоставлении виртуального номера. Кстати, МГТС могла бы предоставлять такую услугу для абонентов электронных АТС, но пока только предоставляет переадресацию внутри своей сети, зато за 14-36 рублей в месяц без ограничений трафика.

У МТС переадресация с повременной оплатой — 0.10\$ в минуту на местные и мобильные телефоны круглосуточно — выгодно при нечастой переадресации и невыгодно при большом трафике переадресованных звонков. У БиЛайн-GSM переадресация стоит 15\$ в месяц, при переадресации на городские телефоны повременной оплаты нет. Переадресацию на телефоны МТС и МСС с 10.12.00 надо еще и повременно оплачивать, а на телефоны БиЛайна в некоторых случаях идет двойная повременная плата — за оба телефона. В МСС стоимость переадресации — в зависимости от тарифа.

Например, на тарифе Рациональный абонентская плата за переадресацию 18\$ без повременной оплаты при переадресации на городские телефоны. В Сонете переадресация стоит 6\$ в месяц без повременной оплаты при переадресации не только на городские, но и на мобильные номера московских операторов.

До 10.12.00 было выгодно пользоваться прямым номером от Билайна для переадресации на городские (МГТС) и мобильные телефоны. Сейчас при переадресации на мобильные телефоны берется повременка, зато можно, к примеру, по тарифу Лидер (абонентская плата 11\$ в месяц) включать переадресацию (18\$ в месяц) на городские телефоны (без повременки). В итоге за 29\$ в месяц получается прямой номер с неограниченным трафиком при переадресации на МГТС. Также для этого можно использовать МСС или Сонет. МСС — к примеру, на тарифе Рациональный —  $36\$ = 18 + 18$  — причем в МСС у вас будет два номера — прямой и кривой. У Сонета самая выгодная переадресация — к примеру, на тарифе Сонет-20 —  $30\$ = 24 + 6$  — причем при переадресации на мобильные московские телефоны повременка не берется.

### Мобильно-МГТС-ный анлим

В случае, если у вас есть возможность часто пользоваться телефонами МГТС, то есть смысл использовать для мобильной связи комбинированный тариф — мобильный+переадресация на МГТС, иногда требуется переадресация на другие мобильные или подмосковные телефоны (Электро-связь-МО). Получается такой своеобразный комбинированный тариф — мобильно-МГТС-ный анлим. Например, я часто бываю дома и еще в паре мест, где могу использовать городские телефоны практически без ограничений (ловить меня по всем телефонам звонящему неудобно), поэтому рассмотрел подобные варианты, предполагая сократить свои расходы примерно раза в три, со 100\$ в месяц на входящем анлиме от МСС с прямым номером ( $89\$ + \text{АОН} + \text{исходящие}$ ). Может, кому еще пригодится.

При переадресации с телефонов Сонета на телефоны других московских ОпСо-Сов не берется повременная плата, только абонентская плата, причем всего 6\$, в Билайне 18\$, в МСС, в основном, тоже 18\$, в МТС абонентской платы за переадресацию нет, но берется повременная оплата даже при переадресации на телефоны МГТС. В АС Сонета удивились моему вопросу про

переадресацию на другие мобильные — «А за что брать деньги, если после переадресации звонка сеть Сонета не используется?». Что тут сказать? Вроде логично, но почему тогда другие ОпСоСы берут за это деньги? Технические особенности или все та же жирная Жаба?

При переадресации с мобильного телефона на другой, АОН на конечном телефоне определяет или мобильный номер инициатора переадресации, или номер абонента, звонящего на мобильный телефон, в зависимости от операторов, наличия услуги АОНа на мобильном телефоне, маршрута звонка и других факторов.

### Тарифные планы

Тарифный план (ТП) — система тарифов и набора услуг. Иногда ТП просто называют тарифом. Абоненты выбирают наиболее подходящие ТП в зависимости от своего трафика, требуемых услуг и других условий пользования. Трафик (traffic) — это эфирное время, то есть время использования телефона, за определенный отрезок времени (как правило, за месяц). Иногда трафиком называют сумму, потраченную на связь за этот период.

ТП бывают повременными и анлимитными (анлим, unlimited).

Повременные — это ТП, на которых оплата идет в зависимости от трафика. Повременные ТП бывают с обязательными платежами (абонентской платой или платой за трафик) и без обязательных платежей. ТП с абонентской платой — МТС-экономный, Билайн-Лидер, МСС-Экономичный и другие, эти ТП составляют большинство предлагаемых операторами ТП. ТП с платой за трафик — МТС-локальный, препейд-ные карточные тарифы (БИ+, МТС-Таксафон, МСС-Секунда — смотри ниже). В карточных ТП плата за трафик присутствует в скрытой форме вследствие ограниченности действия активированной карты. ТП без обязательных платежей в Москве только один — МСС-Разговорный.

### Это сладкое слово — анлим

Анлим — это ТП с абонентской платой и отсутствием повременных платежей. С лета 2000 года московские операторы Сотовой Связи стали активно предлагать анлим. До этого такие ТП предлагал только Сонет. Теперь, анлим есть у всех московских операторов, кроме МТС. Полный анлим — входящие и исходящие местные

звонки (городские и мобильные московских операторов) бесплатные. Квази-анлим (почти-анлим, условный анлим) — это анлим с ограничениями. Например, входящий анлим — входящие звонки бесплатные, исходящие платные. У входящих анлимов есть бесплатный порог (БП), которого вполне хватит для просьбы перезвонить, поэтому часто входящий анлим почти равнозначен полному. Вообще во многих странах входящие звонки и так бесплатны и не являются особенностью какого-либо тарифа, возможно в Москве будет также с введением повременки в МГТС. Временной анлим — анлим в определенные часы.

Конечно, если вы пользуетесь мобильным телефоном только для экстренной связи или ваш трафик не превышает 10 долларов в месяц, то анлим вам не нужен, но для абонентов с большим (да и средним) трафиком уже нет смысла просчитывать минуты и центы, пользуясь повременными ТП, какие бы «экономные» названия у них не были. На самом деле на повременных ТП вопреки рекламе, только молчать можно экономно. А говорить действительно экономно и много (именно так, как навязывается в рекламных образах), не думая о деньгах, можно только на анлиме. Да и ес-

ли ваш трафик меньше стоимости анлима, то учтите, что этот трафик получается, как правило, в результате ужиманий и ограничений, а без них вы бы намного превысили стоимость анлима. К тому же на анлимах не надо заморачиваться по поводу контроля счета, там все просто, как правило, все ограничивается фиксированной абонентской платой.

Анлим у московских операторов (подключение + абонентская плата), на 22.02.01, цены указаны в \$, с НДС или -без НДС (влом пересчитывать за ОпСоСами). Ну и, естественно, без НП.

Билайн-GSM: оплата по кредитной системе, гарантийный взнос 195\$, \$=ЦБ+1%. Периодически на подключение предоставляются скидки.

Corbina: производит подключение к сети Билайн-DAMPs, оплата по кредитной системе, гарантийный взнос 200\$ (явно завышен для тарифа-70), \$=ЦБ+1%.

MCC: \$=ЦБ

MTC: \$=ЦБ

Сонет: На подключение в Сонете периодически предоставляются скидки.

$\$ = \text{ЦБ} + 3\%$  (не жирно?)

При выборе анлима надо обратить внимание на стоимость дополнительных услуг, необходимых вам: АОН, голосовая почта, переадресация, междугородние звонки, роуминг, так как при нужном вам наборе услуг более выгодным может оказаться другой тариф. И, конечно, не надо забывать основные критерии выбора оператора — зона покрытия, наличие связи и ее качество в тех местах, где она вам нужна, ведь если нет связи в тех местах, где вам необходимо, то выгодность тарифов не имеет смысла.

### Кредитные или авансовые?

Тарифные планы делятся на авансовые и кредитные в зависимости от метода оплаты услуг. Особенности этих ТП понятны из их названия. На авансовых ТП надо вносить предоплату. Например, основные ТП МТС, МСС и Сонета — авансовые: деньги есть на счету — говоришь, в минус вышел — будь здоров. Основные ТП Билайна — кредитные, оплата происходит после разговоров, то есть разговоры предоставляются в долг, часто намного превышающий гарантийный взнос, вносимый при подключении.

Кредитная система имеет ряд недостатков:

- Иногда нечистоплотные мелкие и частные дилеры подключают абонентов по чужим паспортным данным. Абоненты выговаривают все деньги на счету, залезают «в глубокий минус» до отключения, а потом владельцам этим паспортов приходят счета, приходится разбираться. Это, так называемое, «подключение на убой».
- Ребенок «поиграл» с телефоном, абонент не рассчитал на отдыхе, да и просто новичок не разобрался с тарифами и наговорил на большую сумму. Конечно, надо быть внимательным, изучать договора и тарифы, следить за детьми, но все же...
- Получение счета по адресу абонента (да и в офисе Билайна или по телефону) доставляет некоторые неудобства для тех абонентов, которые часто переезжают.
- Текущий контроль над расходом средств невозможен, абоненты Билайна на кредитных ТП разговаривают «вслепую», вся информация о рас-

ходах будет только когда придет счет. Нет даже информации о расходе «бесплатных» минут. Хотя это и не является особенностью кредитной системы. Ведь можно было бы и на кредитных ТП сделать автоматизированную систему, аналогичную АССА в МТС, которая бы извещала абонента о его текущих расходах.

Кредитная система накладна для оператора, так как надо тратиться на собирание долгов, а также нести убытки от невыплаченных долгов и «убоя». Эти расходы, кстати, ложатся на плечи остальных абонентов. Кредитная система не оправдала себя у МСС — она раньше тоже допускала большой долг у абонентов (причем даже на авансовых ТП, пользуясь возможностями «привязанных» стандартов), но, видимо, собирать долги стало тяжело, и теперь МСС долга у абонентов не допускает, и даже периодически проводит «долговые амнистии». При кредитной системе надо вносить гарантийный взнос, который, должен возвращаться при разрыве контракта, что тоже хлопотно — надо ехать в офис Билайна, возможно — стоять в очереди, расторгать договор, ждать около двух недель, опять ехать... Кстати, термин — гарантийный взнос —

странное изобретение Билайна, назвали бы уж тогда честнее — «беспроцентная ссуда абонентов Билайну». В исполнении Билайна кредитная система вообще выглядит анекдотично — к примеру, абоненту может прийти текстовое сообщение на телефон (что не адекватно, кстати, «письменному виду» по договору), что ему отключат завтра телефон, хотя крайний срок оплаты счета еще не подошел. Видите ли, в прошлом месяце абонент наговорил больше, чем обычно, и ему надо срочно оплатить счет и увеличить гарантийный взнос, иначе его телефон заблокируют. При этом не важно то, что абонент давний и ранее исправно оплачивал счета. Кстати, если вам заблокируют телефон (и на входящие, и на исходящие), то абонентская плата все равно будет «еще» тикать несколько месяцев, и она будет включена в очередные счета. Лучше долгов не допускать и при разрыве с Билайном (так же как и с другими ОпСоСами и организациями вообще), так как долг будет висеть на вас, будут накручиваться проценты и года через три без малого, возможно, вас будут активно бомбардировать письмами с требованиями об оплате и угрозами подать в суд, что вполне реально. Срок три года, видимо, выбирается для того, чтобы задолженность

выросла, а больше нельзя — по ГК РФ срок исковой давности именно три года.

Для пользования роумингом за границей надо будет увеличивать гарантийный взнос — вносить дополнительную плату за Международный Доступ. Короче, кредит «по-совковому». Кстати, поначалу в МТС тоже была кредитная система (некоторые старые абоненты до сих пор на ней «сидят»), так вот залог абоненту возвращался через несколько месяцев после подтверждения аккуратности абонента в оплате счетов, и далее действовала настоящая кредитная система, когда абоненту предоставлялся кредит на любую сумму разговора безо всяких залогов и жлобских гарантийных взносов. Хотя в МТС в авансовой системе действует так называемый «порог доверия» — при неаккуратном пополнении счета, при выходах в минус, абонент может попасть в категорию, в которой его телефон будут отключать даже при определенном положительном остатке на счету.

Есть и поклонники кредитной системы из-за того, что абонента не отключат, как при авансовой системе, при недостатке денег на счету в самый неподходящий момент), но у МТС на эту ситуацию есть по-

лезная услуга «Обещанный платеж» (0880-131 с мобильного телефона МТС с положительным балансом) — абонент может как бы взять кредит до 10 долларов на этот телефон (точнее — можно будет «уйти в минус» на эту сумму без отключения телефона) с последующей оплатой в течение 7 дней — удобно, если деньги на счету кончаются, а оплатить пока нет возможности. А если носить с собой карту МТС Экспресс-Оплата или у вас есть кредитная карта, таких проблем вообще не будет. Удобство карт ЭО еще и в том, что можно активировать ее на тот телефон, на который более нужно это сделать в данный момент, также удобно картами пополнять свой счет частично для минимизации убытков в случае потери телефона. У МСС тоже есть карты ЭО, к сожалению, их минимальный номинал только 25\$. Пунктов продажи карточек ЭО не так много (как карточек БИ+), а где есть, там постоянные перебои с картами, да и очень мелкий неудобный шрифт в карточках ЭО-МТС, к тому же без пробелов, очень легко ошибиться даже людям с хорошим зрением.

Билайн-GSM начал вводить и авансовую систему. Давно пора. Кстати, тогда будет наглядно видно, какую систему предпочитают абоненты.



Так называемые карточные (предоплатные, предпайдные — pre-paid) ТП — БИ+, МСС-Секунда, МТС-ТАКСАфон — это разновидность авансовых ТП. Преимущество — оплата по картам, четкая система контроля счета, недостаток — нет многих услуг, нет прямых номеров, срок действия карты ограничен (что является обязательной платой за трафик в скрытой форме).

### **Повременные тарифы**

В случае, если ваш трафик небольшой, что вам, конечно, нужен повременный ТП. Здесь надо выбирать в зависимости от ваших потребностей и особенностей операторов и стандартов. Здесь надо считать индивидуально в зависимости от типа звонков: частоты, направления, продолжительности, времени. В случае, если же вам телефон нужен только экстренной связи, то вам нужен тариф без обязательных платежей. Такими тарифами являются МСС-Разговорный и МСС-2+8.

При выборе повременного тарифа замечание для анлимов тоже актуально.

Рекомендации по покупке телефонов

В случае, если вы выбрали стандарт, то можно приступать к выбору телефона. О достоинствах и недостатках различных моделей есть много информации в Internet на форумах по связи и специализированных сайтах по конкретным производителям и модели. Вот некоторые общие рекомендации по покупке GSM-телефона.

Покупайте GSM-900/1800. В случае, если вы выбрали стандарт GSM, то оптимальным вариантом являются двухдиапазонные телефоны GSM-900/1800 — можно будет подключаться и к МТС, и к Билайну-GSM (если в Москве). Тем более, что двухдиапазонные модели ненамного дороже однодиапазонных, да и вообще однодиапазонных телефонов уже выпускается мало. В основном, однодиапазонные телефоны — б/у. С однодиапазонным телефоном GSM-900 в Москве вы сможете подключиться к МТС, и то у вас не будет возможности воспользоваться сетью-1800 там, где она есть у МТС. С телефоном GSM-900 можно подключиться и к Билайну-GSM (неофициально, к примеру, оформив контракт на другой телефон), работать будет почти везде, где и двухдиапазонный. Телефоны GSM-1800 по-

купать нет смысла: в МТС они будут работать только в центре Москвы и некоторых других местах, а у Билайн-GSM сеть-1800 действует только в Москве и Ближнем Подмосковье. В других регионах России тоже, в основном, сети GSM-900, где-то есть GSM-1800 или GSM-900/1800. Опять же — чтобы не забивать себе голову проблемами GSM-роуминга (пользования телефоном в зоне обслуживания другого GSM-Оператора), покупайте телефон GSM-900/1800. Телефоны с GSM-1900 есть смысл покупать только для поездок в США или Канаду, во всех других странах есть GSM-900(/1800) — Штаты и здесь хотели прогнуть весь мир по своей GSM-1900, но на этот раз, обломались.

Не покупайте лоченые телефоны. ОпСоСы и их дилеры иногда продают GSM-телефоны с SP-Lock (или SIM-Lock) — «Service Provider Lock» или «СП-Лох — специально для лохов» (кому как больше нравится), так называемые — лоченые, предназначенные для работы только у конкретного оператора, то есть с SIM-картой конкретного оператора (так называемые «операторские» телефоны), они закодированы для невозможности их использования с SIM-картами других GSM-Операторов. Продают «залочку» не только московские, а

и многие зарубежные GSM-операторы (по различным схемам), но «залочку по-совковому» покупать смысла нет — ОпСоСы скинут (и то не всегда) процентов 10-20 за дешевый телефон и предлагают его абонентам, не акцентируя (естественно) внимание на особенностях лоченых телефонов. А ведь

Закон о ЗПП обязывает продавца это делать, то есть «своевременно предоставлять необходимую и достоверную информацию о товарах, обеспечивающую возможность компетентного выбора». Причем Закон обязывает продавца делать это «в наглядной и доступной форме», так что отмазки в виде галочек в графе «SIM-Lock» не кажутся. МТС на своем сайте предупреждает о залочке информацией, что телефон работает «только с SIM-картой МТС», на сайте Билайна никаких предупреждений нет (и не было), в договоре с абонентом Билайн просто ставит галочку в графе «SIM-Lock». Еще такой момент — почему, к примеру, Билайн-GSM и МТС не предусмотрели официальной процедуры «отвязки» GSM-телефона от оператора? Предположим, что абонент решил перейти из Билайна-GSM к другому GSM-Оператору, официально расторгнул контракт и что? А ничего, легальных путей разлочка телефона Билайн не

предусмотрел, остается только идти к «подпольщикам», которых так не любит сервис-центр Билайна. А это уже похоже на кидняк. Даже в «привязанных» стандартах есть официальная процедура «отвязки» телефона, пусть несколько затянутая, как в NMT-450i, но она есть реально, ей пользуются абоненты для перехода к другому NTM-Оператору. Почему же тогда Билайн пытается «привязать» самый свободный мобильный стандарт GSM? Получается, что он продает одноразовые (в смысле — только для одного оператора) телефоны по неоднократно ценам. А почему бы, к примеру, Билайну (точнее его сервис-центру) официально не разлочивать телефоны (которые залочивают производители по заказу Билайна же), хотя бы тем абонентам, которые официально расторгли контракт с ним? Это было бы правильно со всех точек зрения — юридической, моральной, материальной, технической; у Билайна наверняка есть техническая возможность делать это качественно и получать за это дополнительные деньги.

А сейчас что получается? Деньги за разлочку уходят «подпольщикам» (иногда криворуким), а не Билайну, а у абонента остается злость на Билайн за доставленный

геморрой. Вот, к примеру, казанский GSM-Оператор Сантел официально разлочивает телефоны, «и это правильно»(с). По заверениям своих работников Билайн собирается отказаться от жлобской практики продажи лоченых телефонов. Хорошо, если это так будет на самом деле.

Лучше иметь нелоченый GSM-телефон — у вас будет свобода выбора оператора, мало ли какая будет ситуация, когда нужно подключиться (пусть временно) к другому оператору, то есть просто вставить в свой телефон SIM-карту этого оператора. Например, можно на всякий случай носить с собой SIMку другого оператора, и если вдруг «повис» ваш оператор, то можно воспользоваться связью от другого. Или в другом городе зачастую гораздо дешевле подключиться к местному GSM-Оператору, чем пользоваться роумингом. Единственное неудобство — номер другой будет. Но, по крайней мере, местного оператора можно использовать для местной связи. Да и вообще, если вдруг решили уйти от своего GSM-Оператора к другому, то это легко сделать — просто купить и вставить новую SIMку. С лоченым телефоном всего этого не получится. Телефон на лоченность можно легко проверить, вставив в него поочередно SIM-

карты разных операторов, к примеру, МТС и Билайн-GSM, если телефон будет работать и с тем, и с другим, тогда все нормально — телефон нелоченый (или уже разлоченый). Только надо проверить, выключена ли в телефоне функция работы только с одной SIM-картой, иначе телефон не будет работать вообще с другими SIM-картами (даже того же оператора) без введения кода телефона. Вообще можно купить и лоченый телефон, но, во-первых, гораздо дешевле, чем нелоченый, а, во-вторых, лучше его сразу разлочить на всякий случай. Даже если вы планируете пользоваться только тем оператором, на кого телефон залочен, все равно — мало ли какая возможна ситуация, когда вам будет необходим нелоченый телефон? Телефоны можно разлочить у специалистов за 5-30\$, найти их можно на любой доске объявлений по сотовой связи. Главное — не нарваться на «кулибиных», после которых у телефона могут появиться глюки и неисправности. В любом случае, после этой операции телефон ремонтироваться по гарантии не будет.

Кстати, большая часть новых телефонов, продающихся в московских магазинах по сотовой связи — это ранее залоченные «операторские» телефоны для иностранных

операторов, купленные за границей по дешевке, привезенные и разлоченные здесь, к сожалению, иногда «криво», что может сказаться на дальнейшей работе телефона. Отчасти этим объясняется резкое понижение цен на сотовые телефоны, производителям и их официальным дилерам трудно конкурировать с огромным «серым» потоком телефонов из-за границы. Некоторые производители уже бьют тревогу по этому поводу и пытаются принимать меры. Существуют базы данных по телефонам, официально поставленным в Россию и подлежащие гарантийному ремонту. Например, можно проверить по серийному номеру телефоны Nokia, Benefon, Motorola, Panasonic на сайте МСС-Спектр (справа на странице). Серии номеров телефонов Motorola, официально поставляемых для России можно посмотреть на сайте Motorola, проверить телефоны Motorola по серийному номеру можно и здесь.

Иногда можно услышать или прочитать мнение, что разлоченные (даже правильными руками) телефоны могут некорректно работать, то есть глючить или ломаться. К сожалению, полную информацию на эту тему сложно получить рядовым абонентам. Во-первых, не всегда можно отли-

чить глюки телефона от глюков сети. Во-вторых, нужна достоверная статистика, которую получить трудно. Часто те, кто имеет такую статистику, скрывают или искажают ее, чтобы не навредить своему бизнесу. Например, представители производителей по понятным причинам говорят, что разлочка ведет к порче телефонов (даже если это не так), а анлокеры и торговцы разлочкой утверждают, что правильно разлоченные телефоны работают так же, как и не лоченые ранее. Дискуссии на эту тему постоянно ведутся в Internet. По моему личному опыту, а также опыту моих знакомых — правильно разлоченные телефоны работают так же, как и не лоченые ранее.

Телефоны стандартов NMT-, DAMPS- и CDMA привязаны к оператору, но их можно переподключить, перепрограммировав его у другого оператора. NMT-телефон можно подключить только после процедуры отвязки у своего оператора. DAMPS- и CDMA-телефоны можно подключить без такой отвязки, хотя Билайн лочит некоторые свои DAMPS-телефоны, и их не подключишь. При покупке телефонов «привязанных» стандартов нужна внимательность — по ним ведутся «черные списки». Не обязательно переоформлять телефон на

себя, но желательно взять контракт у старого хозяина.

Телефоны (всех стандартов) еще могут быть закодированные, то есть с секретным кодом, установленным хозяином, и заблокированными — добровольно (хозяином) или принудительно (Оператором по тем или иным причинам). К слову, лучше не кодировать свой телефон (а также желательно снять проверку PIN-кода на SIM-карте GSM-телефона) — в случае потери или кражи телефона есть небольшая вероятность дозвониться на свой телефон новому «владельцу» и договориться о выкупе телефона, в противном случае с телефоном можно распрощаться. В случае потери телефона нужно сразу позвонить своему оператору и попросить заблокировать исходящие звонки.

Телефоны, ранее работавшие в Билайне-GSM. В случае, если купленный вами телефон окажется в «черном списке» Билайна (к примеру, числится как краденый), то этот телефон (и GSM, и DAMPS) не подключат к Билайну. Вы же не всегда можете знать всю историю бэушного телефона, особенно, если он куплен у незнакомых людей, а можете оказаться «крайним».

Можно, конечно, позвонить в Билайн и проверить телефон «на угон», но может получиться так, что в «черном списке» на данный момент телефона нет, но бывший владелец сообщит об этом в Билайн позже. Хотя этот вопрос решается подключением через некоторых нечистоплотных мелких дилеров, которые смотрят на это сквозь пальцы (в погоне за прибылью нарушая правила Билайна) или подключением с другим GSM-телефоном и перестановкой SIM-карты в свой, но все равно — лишние хлопоты. Непонятно, зачем Билайн доставляет абонентам эти неудобства, он же все равно не отслеживает, с каким телефоном работает SIM-карта?

Билайн просто изображает из себя «честного» оператора, но это показная «честность», так как с телефоном из «черного списка» можно подключиться, оформив подключение на другой телефон, а Билайн не контролирует работу таких телефонов в своей сети по IMEI, зачем же тогда такой пафос и ненужные хлопоты для абонентов? Кстати, контроль по IMEI ничего, кроме неудобства абонентам не принесет. У МТС нет «черных списков» («стоп-листов»), так что в МТС можно подключать GSM-телефон без опаски.

Новые телефоны лучше покупать в известных фирмах или в офисах операторов (правда, у операторов цены зачастую завышены), так как гораздо меньше вероятность нарваться на «левый» телефон. В маленьких фирмах-однодневках, которые расположены в подвалах, булочных, уличных ларьках, покупать, во-первых, не очень приятно, а, во-вторых, есть вероятность, что фирма исчезнет вместе со своей «гарантией»? Можно купить телефон и в каком-либо проверенном Internet-магазине с доставкой курьером. Но это подходит только тем, кто твердо знает, какую модель он хочет купить. Тем, кто еще не определился с выбором лучше приехать в хороший магазин с большим ассортиментом и вежливым персоналом, выбрать понравившуюся вам модель, получив грамотную консультацию.

Можно купить и телефон б/у (бывший в употреблении). Здесь уже тактика другая. Главный критерий — минимальная цена, но гарантий никаких, весь риск при покупке бэушного телефона вы берете на себя, этот вариант подходит людям, разбирающимся в телефонах. Лучше покупать б/у-телефоны непосредственно у владельцев, без посредников и фирм, к примеру, в Internet на досках по мобильной связи, по-

падают недорогие б/у-варианты и на радиорынках в Митино или Царицыно. Обязательно надо договориться с продавцом о проверке и возможном возврате в течение хотя бы одного-двух дней (правда, и здесь возможен обман). У бэушного телефона важно проверить (кроме всего остального) аккумулятор, иногда он уже (полу)мертвый. Также желательно проверить (кстати, у нового тоже) соответствие номера IMEI на наклейке под аккумулятором и «прошитого» в GSM-телефоне, набрав на клавиатуре \*#06#. В случае, если номер не совпадает, значит было «хирургическое вмешательство» в телефон: неправильная разлочка, замена радиоблока, замена корпуса. Можно купить и такой телефон, но это хороший повод сбить цену.

В случае, если у вас возникло подозрение, что телефон ворованный, то лучше от такой покупки отказаться, даже если ваши принципы позволяют это сделать. В случае, если телефон «привязаного стандарта», то такой телефон никуда подключить нельзя, так как операторы ведут «черные списки» привязанных телефонов и зачастую обмениваются ими. Некоторые полагают, что в «непривязаном» GSM'е таких проблем нет. Это не так, дело в том, что IMEI GSM-те-

лефона передается по сети оператора, и когда вы вставите вашу SIM-карту в любой телефон и включите его, зарегистрировавшись в сети, то информация из контракта на эту SIM-карту будет сразу известна оператору. В случае, если SIM-карта оформлена на другого человека, то вас все равно можно легко вычислить по звонкам, сделанным вами. С учетом того, что местоположение своего абонента GSM-Операторы определяют с точностью до нескольких сот метров, то вы — как на ладони перед ними, поэтому от сомнительных покупок стоит отказаться.

Вообще, большинство GSM-Операторов не отслеживают телефоны по IMEI, и не блокируют их (и правильно, на мой взгляд, делают), но в особых случаях (если телефон замешан в очень серьезном деле), за вами придут. Потом, скорее всего, разберутся, что вы не причем, но подумайте, нужен ли вам такой геморрой с сомнительным телефоном из-за копеечной экономии?

В случае, если вам надо купить GSM-телефон с подключением, то бэушный телефон покупать нет смысла — дешевле купить новый.

Аксессуары (аккумуляторы, зарядки, чехлы, наушники) можно покупать почти любые, даже «левые», несмотря на понятные протесты производителей и их призывы покупать только «родное». Как показывает опыт, процент отказов таких аксессуаров (а также телефонов из-за них) ненамного выше, чем оригинальных. Хотя по цене оригинальные и неоригинальные аксессуары уже отличаются не так значительно, как раньше, что, кстати, является заслугой «неоригинальных» — если бы не они, цены на оригинальные и сейчас были бы завышенными.

Подключиться с телефоном GSM дешевле и надежнее в офисах операторов, а также у их официальных дилеров, в этом случае активация SIM-карты происходит быстро. У мелких и полуправильных дилеров и субдилеров активация SIM-карты может затянуться на несколько дней, не говоря уже о вероятности откровенного кидняка. У официальных дилеров выгодно покупать GSM-телефоны с подключением — за счет своей комиссии за подключение абонента дилеры снижают цены на телефоны (стоимость новых телефонов получается даже ниже стоимости б/ушных), плюс надо заплатить за подключение. Причем на вашем

счету может оказаться сумма большая, чем вы заплатили за подключение — это тоже нормально, опять же за счет дилерской комиссии, которая немаленькая, поэтому дилерам есть, куда «опускаться». Вообще удивительно, почему МТС и Билайн платят дилерам такую комиссию, зачастую себе в убыток, лишь бы завлечь абонентов. Зачем? Для внушительной статистики?

Нередки случаи кидняка при подключении к операторам, обычно это происходит при обращении к «дилерам» по частным объявлениям. Как правило, сценарий стандартный — вы отдаете сумму за подключение, к примеру, к GSM-Оператору, получаете SIM-карту и договор (липовые) и ждете, но активации SIM-карты не происходит, а «дилер» исчезает. Более того, ваши паспортные данные могут оказаться в «убойных» контрактах (по кредитной системе Билайна), то есть впоследствии операторы будут предъявлять к вам претензии по оплате чужих долгов. В случае подключения к «привязаным» стандартам приходится отдавать на прошивку свой телефон, что чревато потерей не только денег, но и телефона.



Для того, чтобы не было «кидняка», нужно обращаться непосредственно к операторам или к официальным дилерам:

- Дилеры МТС
- Дилеры Билайн-GSM
- Дилеры Сонета
- Дилеры МСС
- Дилеры Билайн-DAMPS

Имейте в виду, что фирмы могут иметь одинаковые названия. Вообще операторам надо бы навести порядок в дилерстве, так как постоянно в Internet и в бумажных СМИ постоянно дают объявления (полу)-левые конторы, не являющиеся дилерами операторов.

Вообще идет заметная тенденция по сокращению полулевых дилеров и торговцев телефонами. В период мобильного бума их расплодилось, как мухоморов после дождя. Сейчас идет снижение темпов «мобилизации», так что в скором времени, видимо, сотовый рынок станет более цивилизованным, останутся только официальные крупные дилеры, поэтому тем, кто хочет остаться в сотовом бизнесе пора уже «ложиться» под кого-либо из них.

### Роуминг

Роуминг — это возможность пользования телефоном вне зоны обслуживания оператора, но в зоне обслуживания другого оператора, с которыми есть роуминговое соглашение. На сегодняшний день пока самый обширный роуминг по России у NMT-Операторов, но GSM-роуминг стремительно развивается. В GSM роуминг автоматический. В случае, если в данном месте есть несколько роуминг-Операторов, то в зависимости от модели телефона и его настроек выбирается или оператор с наиболее сильным уровнем сигнала, или по списку предпочтения, или вручную.

Роуминг — очень удобная и полезная услуга, но без крайней необходимости ею пользоваться не стоит, во всяком случае — пока.

На сегодняшний день роуминговое обслуживание — источник постоянных претензий абонентов к операторам. У Билайн-GSM это еще усугубляется тем, что по кредитным ТП невозможно контролировать свои расходы, счет-сюрприз придет после того, как вы воспользуетесь роумингом, да и у МТС данные из роуминга приходят с некоторой задержкой, то есть в МТС воз-

можно ситуация, когда на вашем счету уже минус, а телефон еще не отключили.

У операторов и роуминг-партнеров зачастую разная информация о тарифах и услугах. Иногда операторы не удосуживаются известить об изменениях своих роуминг-партнеров. Часто в справочниках операторов устаревшая информация, иногда даже неправильные справочные телефоны роуминг-партнера, не говоря уже о тарифах, БП, округлениях и других условиях обслуживания. Вот, к примеру, фрагмент реального ответа на претензию о неправильных удержаниях при роуминге: «... АО «Вымпелком» не может гарантировать точность информации, предоставленной компанией-оператором, оказывающим услуги роуминга. Данная информация постоянно изменяется и зависит от услуг, предоставляемых оператором «гостевой сети»».

У некоторых региональных операторов значение условных единиц занижено (якобы дешево), к примеру, у Кубань-GSM сейчас почему-то «уе» равен 21 рублю, что вносит дополнительную путаницу в пересчете тарифов. При входящем звонке в роуминге стоимость минуты разговора складывается из двух составляющих: платы за

междугороднюю связь в сети МТС и платы за входящий звонок, которую устанавливает местный оператор (иногда она не берется). Так же надо учесть особенности хитрой тарификации при роуминге таких услуг, как голосовая почта и переадресация, лучше вообще выключить все установки переадресации на период пользования роумингом.

Изучать всю эту информацию у абонента не всегда есть возможность, особенно тем, кто постоянно перемещается. Не у всех абонентов есть возможность постоянно следить за условиями операторов и выбирать оптимального для роуминга. Сложность «разборов полетов» в том, что операторы для прояснения информации отсылают по месту получения услуг связи, то есть к роуминг-партнеру. Получается — концы в воду, так как мало кто из абонентов этим будет заниматься. Например, у кого-то из операторов почему-то нет БП, кто-то (к примеру, самостийный Киевстар-GSM) берет деньги за несостоявшийся разговор — за сообщение автоответчика о том, что абонент (то есть — вы) недоступен. Вот это «отличный» сервис — пока вы недоступны (к примеру, находитесь в метро), то ваши деньги списываются, причем, по роуминговым тарифам, если вам пытаются дозво-

ниться. Кто-то из операторов (российских!) установил запредельные тарифы. Например, звонки в Москву у многих операторов достигают 2-2,5\$ за минуту (причем не обязательно из дальних регионов), да и местные звонки у некоторых роуминг-Операторов примерно такие же, а, к примеру, в Хабаровске и Новосибирске местные звонки (если пользоваться услугами Северо-Западного GSM) для абонентов МТС стоят около 3.60\$ за минуту! Лучше, по возможности, воспользоваться услугами других роуминг-партнеров МТС, соответственно ДСС (Дальневосточные Сотовые Системы) и CCC (<http://www.scs-900.ru/welcome.html>) (Сибирские Сотовые Системы), в этом случае звонок обойдется в несколько раз дешевле, но в конкретном месте может лучше работать другой оператор. В данном случае, нужного вам оператора лучше установить вручную.

Неудачных примеров пользования роумингом много, об этом свидетельствуют многочисленные жалобы абонентов на неправильное (или непонятное) списание денег при использовании роумингом. Хорошо, если находится дотошный абонент, который обращает внимание на это несоответствие, а сколько еще таких «неточностей»

не в пользу, естественно, абонента, которые пока никем не замечены? Так что лучше не пользоваться роумингом без крайней необходимости, а если уж без этого нельзя, то постарайтесь получить максимальную информацию о тарифах и условиях роуминга в тех регионах, куда вы собираетесь, но и это, правда, не является гарантией отсутствия недоразумений при использовании роумингом.

### Радиотелефоны

Можно пользоваться связью без участия ОпСоСов -купить радиотелефон дальнего действия (РДД), так называемых радиоудлинитель (РУ) — Senao, Harvest и другие, которые подключаются на обычную телефонную линию, к примеру, МГТС, со всеми вытекающими из этого радостями (для абонента, но не для ОпСоСов и чиновников, который с этого ничего не имеют). Не всем, конечно, этот вариант подойдет, но в ряде случаев это удачное решение (можно как дополнительный вариант связи). Например, если ваша деятельность, в основном, протекает в радиусе нескольких километров от дома. Также можно рядом с нужным местом найти пенсионерку, кото-

рая за небольшие деньги сдаст вам свой телефон в аренду, и вы за эти деньги будете иметь круглосуточный анлим. Хотя сейчас и ОпСоСов тарифы понизились, в том числе и на анлим, но все равно еще дорого, да и жлобские замашки ОпСоСов раздражают. Плюсы РДД очевидны: платите только один раз за сам телефон (200-1500\$), а минусы такие:

- большой размер (15-25см) и вес (200-500г) трубок, (хотя последние РУ типа Senao-358 имеют габариты и дизайн сотовых телефонов. Более того, сейчас выпускаются РДД в корпусах сотовых телефонов.
- возможность пиратского подключения к вашему телефону, хотя это решается небольшим вложением денег на защиту.
- ограниченная зона действия (1-100км), искусственная нелегальность (спасибо МинСвязи). Главное условие для использования РДД — возможность установки внешней антенны как можно выше (желательно на крышу дома), в противном случае дальность и качество связи будут невысокие.

- нельзя пользоваться в других городах, хотя разорительный роуминг у ОпСоСов тоже не каждому подойдет. Некоторые переделывают РДД на сканеры с возможностью использования в любом городе мира, цепляясь за чужой телефон, но это уже нехорошо.

Так почему же некоторые РДД не решить к использованию в РФ, хотя бы маломощных? Ответ очевиден — это невыгодно ОпСоСам и чиновникам от связи, многие из которых имеют свой интерес в различных организациях связи. Ссылки на запрещенные частоты неубедительны. ОпСоСы тоже потеряют часть трафика при разрешении и развитии РДД. Нет свободных частот? Возможно, но это уже вопрос из другой области. Большая часть спектра частот в нашей стране занята под военные «нужды». В случае, если посмотреть реестр выделенных частот, что там почти все занято различными НИИ, НПО. Значительная часть из них используется неэффективно. Какой-нибудь «почтовый ящик» уже давно кастрюли выпускает вместо ракет, а частоты у него остались, и отдавать их они не собираются. Грудью будут стоять. Частоты для некоторых военных — это как нежилые помещения для бюджетных организаций,

можно использовать в корыстных целях. Постоянно на эту тему всплывают «нехорошие истории», недавний пример из СМИ — высокопоставленный чин в Генштабе был взят с поличным за взятку за улаживание вопроса в региональном частотном конфликте между военной частью и местным телевидением. А сколько таких историй было бы известно, если бы не якобы «военная тайна»? А сколько таких ситуаций решают за взятки, о которых никто не знает?

Да что далеко ходить, достаточно вспомнить громкий частотный скандал в 900-мегагерцовом диапазоне для нового GSM-Оператора в Москве Соник Дуо? Не удалось (пока?) отобрать их у МТС и Билайн, и пошли переговоры с военными, которые тоже плотно сидят и 900-мегагерцовом диапазоне (в какой еще стране сотовый диапазон 900-МГц занят под военные «нужды»?) Так вот пока военных не удалось «сдвинуть» с этого диапазона даже мощными усилиями лobbyистов Соник Дуо, которые, по сообщениям некоторых источников, есть в самых высоких кабинетах. Так что военные будут до конца упираться, и частоты у них отобрать будет очень сложно. Ситуация с «военными частотами» настолько назрела, что даже министр связи РФ Ле-

онид Рейман «намерен заняться конверсией радиочастотного спектра». Рейман отметил, что «сейчас лишь 4% спектра используется для гражданских средств, еще 20% находятся в совместном применении. Работа по высвобождению ресурса — занятие дорогостоящее, военные идут на него с неохотой, а источники финансирования так до конца и не определены».

В 1998 году произошел сдвиг: сертифицировали и разрешили к использованию в России РДД Senao SN-868R — платишь какие-то деньги за регистрацию и вперед. Правда, их использование разрешено только в пригородных и сельских районах, в крупных городах запрещено. Видимо, их разрешили для того, чтобы была связь в глухой тайге. Ну хоть что-то, но тщетно надеяться на то, что будут разрешены другие РДД. Хотя, в связи с навигацией повремени, у РДД может появиться мощный лobbyист — МГТС. А пока можно проводить акции гражданского неповиновения в области связи — покупать РДД и пользоваться ими, если есть необходимость в этом.

Какие возможны санкции? По КоАП пользование РДД запрещено. В реальности — никто не будет заниматься вами, если вы

используете РДД небольшой мощности, если, конечно, случайно не окажется, что то самое НПО находится в соседнем с вашим доме. Ну и, конечно, если вы будете использовать РДД на вашей даче, которая находится, к примеру, недалеко от Шереметьева, а база будет на московской квартире, то вас быстро «вычислят» (кстати, это тоже реальная ситуация из СМИ). В других случаях никто вами специально заниматься не будет. На улице тоже ходить безопасно в этом плане — в связи с отменой разрешения на сотовые телефоны у милиционеров пропал рефлекс на человека с телефоном в руке. Так что подумайте, может это то, что вам нужно, по крайней мере, в комбинированном варианте — пользоваться и сотовым телефоном, и РДД, в зависимости от необходимости и конкретной ситуации.

Есть еще вариант покупки радиоудлинителя для домашних радиотелефонов 900 МГц, к примеру Panasonic. Этот вариант безопасный, так как эти телефоны разрешены, а то, что они будут работать через радиоудлинитель, определить сложно. Варианты таких радиоудлинителей есть здесь или здесь.

В России (также как и во всем мире) разрешен стандарт DECT — не РДД, конечно, но тоже полезный. Дальность связи: до 50м в помещениях и до 300м на открытой местности. Дополнительные применения: есть телефоны-гибриды GSM+DECT, такие модели есть у компаний Sagem и Ericsson. Странно, что моделей GSM+DECT нет у Siemens — одного из лидеров и GSM-, и DECT-связи. Также интересны варианты создания собственной DECT-сети.

### Радиосредства

Итак, все эти средства, обеспечивая возможность оперативной связи, значительно расширяют наши возможности. Речь, конечно, идет не о том, что все эти средства можно использовать и для несанкционированного доступа к конфиденциальной информации (для подслушивания, подсматривания и передачи информации, для доступа в компьютеры и линии связи, копирования информации, внесения исправлений и нарушения работы и т.д.). Однако, существует достаточно много других возможностей для применения приведенных (или аналогичных) средств.

Необходимо всегда помнить, что для специальных целей недопустимо использовать радиовещательные диапазоны.

Средства связи можно использовать в составе систем охранной сигнализации. Для этой цели некоторые схмотехнические решения используются достаточно активно. И это правильно, и это нужно, и это достойно. В составе этих охранных устройств можно использовать приведенные миниатюрные (скрытное использование для сигнализации) приемники и передатчики. К КВ-или УКВ-передатчику подключаются датчики охранной сигнализации, контроль над ними осуществляется посредством соответствующего радиоприемника. Расстояние, как правило, составляет всего несколько десятков метров. В этом случае используются маломощные передатчики, но с целью увеличения дальности могут использоваться и мощные устройства. Обычно для этих целей применяют АМ-передатчики.

Родители, имеющие маленьких детей, по достоинству могут оценить устройства, облегчающие дистанционный контроль. Малогабаритный микрофон, подключаемый с помощью экранированных проводов к миниатюрному усилителю на одном-двух

ОУ (можно использовать двоянные ОУ), провода и громкоговоритель (динамик) могут существенно облегчить жизнь.

Эти же схемы устройств можно использовать в охранных целях. Микрофон помещается в контролируемом помещении, а громкоговоритель располагается, конечно, в другом месте: там, где осуществляется прослушивание. При этом прослушивание может быть периодическим или постоянным.

Теперь о возможных вариантах реализации подобных систем.

Первый вариант. Усилитель и громкоговоритель (динамик) расположены вместе, а микрофон расположен у источника звука (например, в детской комнате) на расстоянии 5-10-20 м. При таком значительном удалении целесообразно микрофон подключать к дифференциальному входу усилителя. Подключение микрофона к усилителю следует осуществлять с помощью экранированных проводов. Такая структура системы целесообразна в тех случаях, когда источник электропитания электронной схемы усилителя (УНЧ) находится в месте расположения громкоговорителя.

Второй вариант. Микрофон и усилитель расположены вместе у источника звука, а громкоговоритель на расстоянии 5-10-20 м. При "низ-коомном выходе" усилителя, что является типичным для усилителей на ОУ, проблем с таким включением, как правило, нет. Способ подключения микрофона к усилителю зависит от расстояния между ними и условий эксплуатации, например, от величины окружающих электромагнитных помех. При значительном удалении (более 0.5 м) микрофон следует подключать к усилителю с помощью экранированных проводов. При удалении более 1 м лучше использовать дифференциальный вход усилителя. Если сравнивать с первым вариантом, то предложенная структура системы характеризуется меньшим уровнем внешних помех (основная помеха - фон 50 Гц и 100 Гц). Она целесообразна в тех случаях, когда источник электропитания находится в месте расположения микрофона.

Третий вариант. Этот вариант предусматривает наличие двух усилителей: один - у микрофона, другой - у громкоговорителя. Такую структуру часто выбирают, когда не хотят передавать сигнал низкого уровня (микрофонного) на значительные расстояния. В этом случае осуществляется переда-

ча сигнала после предварительного усиления, т.е. передача сигнала значительно большего уровня (после ОУ полезный сигнал может быть усилен до уровня в несколько вольт). Такой сигнал можно передавать на значительные расстояния, например, в десятки и даже сотни метров. Имеются схемы, обеспечивающие передачу питания для предварительного усилителя по сигнальным проводам, соединяющим выход первого усилителя со входом второго.

Монтаж и настройка. Настройка усилителей сводится к установке требуемых коэффициентов усиления и минимизации уровня синфазных помех в дифференциальных каскадах, а выбор конкретного варианта схемы зависит от поставленных задач.

Интересные варианты различных охранных систем могут быть получены при включении в перечисленные электронные структуры разнообразных радиопередающих и радиоприемных средств: передатчиков, приемников, конвертеров и т.д. Так, например, после микрофонного усилителя можно включить передатчик, а перед усилителем с громкоговорителем установить соответствующий радиоприемник. Подобная структура, использующая радиопереда-



ющие средства, позволяет обойтись без проводов. Это повышает мобильность устройства контроля, в состав которого входят микрофон, передатчик и передающая антенна. Радиоприемный тракт может иметь в своем составе специализированную приемную антенну, антенный усилитель, конвертер и т.д.

Такое устройство можно установить, например, в детской коляске. Это позволит родителям осуществлять постоянный контроль над ребенком. При этом часто достаточно мощности передатчика в несколько мВт - мощности, достаточной для обеспечения радиопередачи на несколько десятков метров. Этого расстояния достаточно для осуществления контроля над ребенком, например, при посещении магазинов.

Подобное миниатюрное устройство можно установить, например, в автомобиле. Если такое устройство периодически (автоматически) включать и выключать, то оно превращается в своеобразный радиомаяк. Угнанный автомобиль (или другая не менее дорогая вещь) с работающим радиомаяком можно запеленговать обычным образом.

Эксплуатация радиопередающих средств предусматривает предварительное получение разрешений в соответствующих инстанциях.

Можно придумать и предложить достаточно большое количество различных примеров использования приведенных устройств. Некоторые из вариантов могут быть даже неожиданными, что, кстати, не уменьшает их функционального значения.

Например, миниатюрный УКВ ЧМ-радиопередатчик можно использовать для расширения функциональных возможностей бытовой радиоаппаратуры. С помощью такого устройства можно обеспечить возможность записи на магнитофон, входящий в состав магнитола, не имеющей отдельного входа записи. Стандартная ситуация, характерная для относительно дешевых устройств. Отсутствие отдельного входа записи не позволяет осуществлять запись от другого источника сигнала, например, от другого магнитофона, от CD-плеера, от проигрывателя граммофонных (виниловых) пластинок и т.д. Для таких магнитол запись на магнитофон возможна только с микрофона (чаще - встроенного или реже - внешнего) или от встроенного УКВ-радиоприемника.

Однако эту проблему можно решить. И достаточно просто. Сигнал для записи (на магнитофон) от внешнего источника подается на УКВ ЧМ-радиопередатчик, далее - принимается УКВ ЧМ-радиоприемником, входящим в состав магнитолы, и записывается на магнитофон уже с УКВ ЧМ-радиоприемника стандартным образом. Благодаря ЧМ-модуляции достигается высокое качество записи. Для записи ЧМ-радиопередатчик используется маломощный - достаточно мощности в 1 мВт и даже менее. Это может быть ЧМ-радиопередатчик как на биполярном транзисторе, так и на МОП-транзисторе или даже на туннельном диоде. В качестве радиопередатчика может быть использована одна из описанных ранее конструкций. Уменьшение мощности излучения, а она должна быть минимальной (для уменьшения излучения в окружающее пространство), можно достичь использованием на выходе ЧМ-передатчика конденсатора (связи) малой емкости: 1-10 пФ. Непосредственное соединение выхода используемого радиопередатчика (через конденсатор или катушку связи) с телескопической антенной ЧМ-радиоприемника при использовании хорошего экранирования обеспечит хорошую электромагнитную совместимость

с радиоприемными средствами, которые могут находиться рядом - другой УКВ-радиоприемник, телевизор и т.д. Хорошая экранировка обеспечивается использованием металлического корпуса (лучше, если медного) для УКВ ЧМ-передатчика. Корпус-экран соединяют с "заземленным" контактом источника питания данного передатчика. Антенна УКВ-приемника, с которой соединяется выход передатчика, должна иметь, конечно, минимальную длину.

При малой мощности излучения радиопередатчика, экранировании и короткой антенне УКВ-радиоприемника использование данного метода не внесет существенных радиопомех даже на коротком расстоянии (несколько метров).

### Индукционные передатчики и приемники

Такой передатчик и контур, расположенный по периметру квартиры, подключенные к источнику сигнала, например, к телевизору, магнитофону, радиокомплексу и т. д., обеспечивают дистанционное (беспроводное) прослушивание этих устройств с достаточно хорошим качеством.

Очевидно, что индукционных приемников может быть несколько.

Такой же индукционный передатчик и соответствующим образом расположенный контур могут обеспечить передачу информации (НЧ-сигналов) через препятствия, например, одну или даже две-три квартиры. Использование передатчиков и приемников с каждой из сторон (два индукционных передатчика, два или несколько индукционных приемников) обеспечивают дуплексную связь. Использование селективных фильтров позволяет повысить дальность устойчивой связи. В качестве таких фильтров можно использовать многополосные регуляторы тембра. Это могут быть двух-, трех-, пятиполосные регуляторы (и более).

Приемники индукционной связи можно использовать в системах, обеспечивающих усиление и громкоговорящую трансляцию телефона, что позволяет расширить его функциональные возможности.

Индукционные устройства могут быть использованы не только в качестве устройств связи, обеспечивающих одностороннюю или двухстороннюю связь. Например, описанные индукционные приемники

практически без всякой переделки можно применить для поиска электрических проводов при их скрытой проводке.

### Globalstar

Одной из наиболее заметных тенденций в развитии телефонии в последнее десятилетие является быстрый рост числа абонентов сотовой связи. За 26 лет, прошедших от момента зарождения идеи до настоящего времени, число абонентов, пользующихся услугами сотовых систем, достигло 200 млн, а к 2001-2002 годам оно увеличится до 500-600 миллионов. Однако возможность эффективного построения наземных сотовых систем существует далеко не везде, и альтернативным вариантом — особенно для предоставления телекоммуникационных услуг в труднодоступных и малонаселенных районах — является применение спутниковых систем персональной связи (ССПС).

Идея построения ССПС состоит в использовании методов сотовой связи, но с размещением ретрансляторов базовых станций в космическом пространстве. В результате зона обслуживания одной станции многократно увеличивается, и появляется

возможность создания на базе искусственных спутников Земли (ИСЗ) глобальной системы, обеспечивающей пользователя связью в любой точке планеты. Сочетание наземных и спутниковых систем персональной связи и их интеграция обеспечат возможность приема и передачи речи, данных и факсимильных сообщений в любом регионе Земли с приемлемым уровнем цен на предоставляемые услуги.

Globalstar — это глобальная цифровая система персональной связи, основанная на использовании низкоорбитальных спутников. При разработке системы Globalstar был использован опыт создания сотовых систем связи с кодовым разделением каналов фирмы QUALCOMM, Inc. Набор услуг системы Globalstar в целом аналогичен услугам ССПС Iridium и включает передачу речи, данных, факсимильных сообщений, сигналов персонального радиовызова (пейджинговых сообщений) и, кроме того, — определение координат подвижных объектов. Следует отметить, что система предназначена для абонентов не только мобильной, но и обычной связи.

Так же, как в ССПС Iridium, прежде чем установить связь, мобильный терминал

Globalstar должен будет сначала проверить возможность работы в наземной сотовой сети связи и лишь при невозможности этого будет устанавливаться соединение через спутник.

В этом случае сигнал с абонентского терминала (телефонного аппарата пользователя) будет передаваться через спутник на ближайшую земную станцию сопряжения, которая соединит его с требуемым абонентом обычной телефонной сети, сотовой сети или с абонентом системы Globalstar. Принцип действия системы иллюстрируется на рис. 1. При этом максимальная задержка сигнала не должна превышать 150 мс, а время установления соединения — 5 с. Мировой роуминг позволит дозвониться до абонента по одному и тому же номеру, вне зависимости от его географического местоположения.

При передаче речи исходный сигнал преобразуется в цифровую форму с помощью адаптивного вокодера с линейным предсказанием (CELP), создающего трафик от 1,2 до 9,6 Кбит/с (средняя скорость для данного алгоритма приблизительно равна 2,4 Кбит/с). Вокодеры, установленные на земных станциях, включают в свой состав

эхоподавители. Качество передачи речи при этом, по средней оценке мнений (MOS), эквивалентно цифровым сотовым системам. Цифровые данные передаются со скоростью до 9600 бит/с, что заметно выше, чем в ССПС Iridium (до 2400 бит/с).

Вероятность ошибки при этом не превышает 10<sup>-6</sup>.

Предполагаемыми абонентами Globalstar станут люди, совершающие частые поездки и нуждающиеся в глобальной беспроводной коммуникационной системе.

Для реализации ССПС Globalstar в 1991 году компаниями Loral Aerospace Corporation (Нью-Йорк) и QUALCOMM Incorporated (Сан-Диего, шт. Калифорния) был создан консорциум Globalstar Limited Partnership. В него вошли также ведущие международные фирмы — производители спутниковых систем и телекоммуникационного оборудования — Elsat (Италия), Alenia (Италия), Alcatel (Франция), Hyundai Electronics Industries (Южная Корея), DACOM (Южная Корея) и операторы связи — France Telecom (Франция), AirTouch Communications (США), Vodafone Group (Великобритания). В работе по реализации проекта активное участие принимает груп-

па Alliance. К изготовлению спутниковых платформ привлечена компания Space Systems/Loral (Пало Альто, шт. Калифорния). Парижская фирма Alcatel Espace изготавливает для каждого ИСЗ полезную нагрузку, в том числе остроуправляемые антенны. Корпорация QUALCOMM отвечает за разработку абонентской аппаратуры и оборудования для наземных центров управления, которое обеспечит связь спутников с наземными сетями. Итальянской компанией Alenia в Риме еще в 1997 году было построено и официально введено в строй предприятие по сборке, комплектации и испытаниям космических аппаратов (КА).

Компания Air Touch Communications будет предоставлять услуги спутниковой связи на территории США. Также в проекте участвуют фирмы Finmeccanica/Elsag Bailey Company (Италия), DASA (Deutsche Aerospace AG/Daimler-Benz AG, Германия), Aérospatiale (Франция), China Telecom и др. Общая стоимость системы, включая космический и наземный сегменты, оценивается приблизительно в 2,6 млрд. долл. США. Годовые эксплуатационные расходы должны составить 227 млн. долларов.

Система Globalstar включает три основных сегмента: космический (космические аппараты), наземный (земные станции контроля, управления и сопряжения) и сегмент пользователя (терминальные устройства). Рассмотрим их более подробно.

В соответствии с проектом космический сегмент должен состоять из 48 основных ИСЗ и 4 резервных (что гораздо меньше, чем в ССПС Iridium), расположенных на 8 орбитах — по 6 основных ИСЗ на каждой (рис. 2). Орбиты — наклонные, круговые с наклоном к экватору —  $52^\circ$  (в отличие от полярных орбит с наклоном  $86^\circ$  в ССПС Iridium), что сужает ширину зоны обслуживания системы в целом. Период обращения ИСЗ на орбите равен 113 мин. Высота орбит составляет 1414 км (почти в два раза выше, чем высота орбит ИСЗ Iridium). Большая высота орбиты обуславливает, с одной стороны, большую зону обслуживания каждого ИСЗ и больший срок службы КА (7,5 лет), с другой, — большее запаздывание и затухание сигнала, более дорогой вывод спутника на орбиту.

Космический сегмент построен так, чтобы обеспечить наилучшее обслуживание пользователей в средних широтах. Именно

в средних широтах доступными являются не менее двух КА. Ширина всей зоны обслуживания ограничена  $70^\circ$  северной и южной широты. Поэтому в Антарктиде, на Северном полюсе, в северных регионах России и Гренландии, в некоторых районах Северного морского пути пользование системой Globalstar невозможно. В ССПС Iridium подобной проблемы не возникает.

Одной из важных характеристик спутниковых систем персональной связи, влияющих на качество соединения и доступность системы, является минимальный угол возвышения ИСЗ над поверхностью Земли. При большом угле возвышения сигналы от спутника к Земле должны пройти через меньший слой земной атмосферы, влияющий на затухание сигнала, а всевозможные препятствия на Земле (горы, растительность, строения) будут оказывать меньшее воздействие. Требования к минимальному углу возвышения определяют число спутников в системе. Для полярных орбит число спутников выбирается исходя из необходимости покрытия экваториальных районов, так как пересечение орбит на полюсах приводит к существенному переполнению емкости системы в этих местах. В ССПС Iridium минимальный угол возвышения у

экватора равен  $8^\circ$ , а в системе Globalstar в экваториальных районах минимальный угол возвышения составляет  $15-20^\circ$ , что способствует более качественному обслуживанию пользователей.

ИСЗ Globalstar представляет собой ретранслятор с преобразованием частот, который осуществляет прием сигналов в пределах зоны обслуживания, их преобразование и передачу на земную станцию. Все операции по обработке вызовов, их коммутации, преобразованию сигналов и разделению каналов производятся на Земле, где реализация данных функций обходится дешевле, аппаратура доступна для технического обслуживания и может быть со временем модернизирована. Отсутствие обработки сигнала на борту КА, а также отсутствие в системе Globalstar линий межспутниковой связи (в отличие от ССПС Iridium) делают КА проще и надежнее.

На спутниках Globalstar предусмотрена трехосная система стабилизации. Вес ИСЗ — около 450 кг. Солнечные батареи имеют мощность 1100 Вт. Мощность передающей системы ИСЗ приблизительно равна одному киловатту. За счет оперативной регулировки потребляемой мощности бор-

тового ретранслятора в каждом канале в соответствии с условиями приема минимизируются энергетические ресурсы ИСЗ.

Для связи с земными станциями (фидерные линии связи) на спутниках устанавливаются по две рупорные антенны (для приема и передачи), работающие в С-диапазоне частот (5091-5250 МГц для линии “вверх” Земля-ИСЗ и 6875-7055 МГц для линии “вниз” ИСЗ-Земля). Этот диапазон за счет применения правой и левой круговой поляризации будет использоваться дважды.

Для линий связи ИСЗ с мобильными пользователями предусмотрена эксплуатация частот L-диапазона (1610-1626,5 МГц) для линии “вверх” абонент-ИСЗ и S-диапазона (2483,5-2500 МГц) для линии “вниз” ИСЗ-абонент. Антенны L- и S-диапазонов представляют собой активные фазированные антенные решетки (ФАР) с 16 лучами. Каждый луч (лепесток) имеет свою зону обслуживания на поверхности Земли площадью приблизительно 2,9 млн. км<sup>2</sup>. Совокупность лучей образует зону обслуживания ИСЗ, близкую по форме к кругу диаметром 7600 км. Приемная антенна (L-диапазон) состоит из 61 элемента. Передающая ФАР

(S-диапазон) возбуждается 91 печатным усилительным элементом мощностью 4 Вт каждый. Общая мощность ИСЗ в S-диапазоне достигает 400 Вт и может плавно перераспределяться между лучами.

Для уплотнения телефонных каналов в системе Globalstar будет использоваться комбинация методов многостанционного доступа с частотным и кодовым разделением каналов (МДЧР и МДКР). Общая полоса частот шириной 16,5 МГц, отведенная для связи в L- и S-диапазонах, разделена на 13 поддиапазонов шириной 1,25 МГц, в каждом из которых выполняется кодовое уплотнение сигналов от нескольких (порядка 50) абонентов. Для этого сигнал абонента преобразуется в широкополосный сигнал (1,25 МГц).

Широкополосные сигналы в отличие от узкополосных позволяют существенно снизить требования к развязке между соседними лучами многолучевой антенны. Такие сигналы обеспечивают мягкую перегрузку, то есть превышение номинальной загрузки не приводит к отказу, а лишь несколько снижает на короткое время качество передачи каждого сигнала, что обычно считается допустимым. Применение МДКР позво-

ляет изящно решить проблему переключения абонента с заходящего спутника на восходящий. Как только происходит снижение уровня пилот-сигнала во время работы абонента в каком-либо луче, терминал по команде станции сопряжения автоматически переключается на двухканальный режим работы, в котором обеспечивается одновременный прием и когерентное сложение сигналов от двух разных лучей или от разных спутников. Через некоторое время поступает команда на отключение первого луча, и обмен информацией производится только через второй луч. Какое-то время сигнал от абонента принимается и передается одновременно с двух спутников, а земные станции обрабатывают суммарный сигнал, что делает процесс переключения спутников незаметным для пользователя. Такая технология — возможность когерентного сложения сигналов от нескольких спутников в приемном устройстве пользователя — позволяет также уменьшить влияние затенения от препятствий на поверхности Земли. К недостаткам МДКР следует отнести тот факт, что использование широкополосных сигналов усложняет оборудование пользовательских терминалов и увеличивает время вхождения в зону связи.



За счет МДКР, учета речевой активности и применения многолучевой антенны обеспечивается повторное использование частот, в результате чего каждый ИСЗ способен к одновременной ретрансляции около двух тысяч телефонных каналов. При этом на 1 миллион км<sup>2</sup> поверхности Земли ИСЗ Globalstar одновременно обеспечивает всего несколько десятков каналов связи, что еще раз подтверждает тот факт, что спутниковые системы персональной связи в отличие от наземных сотовых систем не ориентированы на использование в густонаселенных районах.

Наземный сегмент ССПС Globalstar включает земные станции сопряжения, а также центры управления и контроля орбитальной группировкой (Satellite Operations Control Center) и наземными средствами (Ground Operations Control Center). Центр управления и контроля орбитальной группировки на основе телеметрической информации контролирует текущее состояние ИСЗ и параметры их орбит, при необходимости выдает соответствующие команды. Центр управления и контроля наземных средств отвечает за планирование и распределение ресурсов системы, контроль за ее функционированием. Центры будут распо-

ложены на территории США и связаны между собой и с другими земными станциями системы с помощью специальной сети передачи данных GDN (Globalstar Data Network).

Поскольку система Globalstar в большей степени ориентирована на интеграцию с существующими наземными телекоммуникационными инфраструктурами, станции сопряжения являются в ней основными коммуникационными элементами. Фактически земные станции сопряжения являются шлюзами, на которые возложены функции обеспечения интерфейса с существующими и будущими телекоммуникационными системами, в частности с наземными телефонными сетями общего пользования и сотовыми системами связи в зоне обслуживания каждого ИСЗ. Все вызовы (местные и международные) должны обрабатываться и коммутироваться на станции сопряжения. В этом состоит так называемый региональный принцип построения связи — обязателен выход каждого абонента на ближайшую станцию сопряжения и далее — на существующую фиксированную сеть или на связь с другим абонентом. Таким образом, в организации любого соединения участвуют земные станции. Поскольку основную

часть трафика в каждом регионе обычно составляют местные вызовы (более 80%), такое решение выглядит весьма рациональным, облегчает связь с абонентами сетей общего пользования, укорачивая трассу для основной массы соединений, а также позволяет сделать систему частью национальной сети каждой страны, что привлекает операторов связи, позволяя им получать дополнительные доходы.

С другой стороны, так как в системе задействовано большое число земных станций сопряжения, соединения становятся зависящими от состояния наземных сетей. Для глобального покрытия земной поверхности (в пределах 70° северной широты — 70° южной широты) с учетом национальных границ и минимизации наземного трафика, по оценкам разработчиков Globalstar, потребуется 150-210 станций сопряжения, в том числе 9 — на территории России. Типовая станция сопряжения содержит 4 идентичные следающие параболические антенны с диаметром рефлектора 5,5 м с левой и правой круговой поляризацией и стоит около 5,5 млн. долл.

На стыке земной станции с наземными сетями общего пользования используется стандартный интерфейс T-1/E-1 и системы сигнализации R1, R2 и №7.

Сегмент пользователя системы Globalstar может включать один из трех основных типов терминалов: портативные (аналогичные сотовым), мобильные (устанавливаемые в автомобилях или других транспортных средствах) и стационарные (телефонные аппараты, таксофоны). Последовательный порт ввода/вывода данных позволит подключать к терминалам пользователя компьютер, факсимильный аппарат или другие внешние устройства и обеспечивать передачу данных или факсимильных сообщений. Предусматривается адаптивное управление мощностью передатчика терминала.

Портативные и мобильные аппараты оборудованы ненаправленными антеннами и могут функционировать также в наземной сотовой сети стандарта GSM, AMPS или IS-95.

Терминалы Globalstar, работающие более чем в одном режиме, должны сначала проверить возможность работы в наземной сети персональной радиосвязи и, если

это невозможно, попытаться установить соединение через спутник. При переходе таких терминалов от режима работы в сотовой сети связи в режим работы в системе Globalstar автоматическое переключение не предусматривается. Если абонент покинул зону действия сотовой сети, связь будет прервана и для ее восстановления необходимо будет вновь запросить соединение, но уже в ССПС Globalstar.

Вес портативного терминала — около 350 г, размеры 190 x 60 x 30 мм, а его мощность не превышает 0,6 Вт. Заряда аккумулятора при работе в режиме системы Globalstar будет хватать на 8 часов дежурного приема и на 1 час разговора. В режиме наземной сотовой системы связи продолжительность его работы увеличится до 12 час дежурного приема и 2 час разговора (или даже больше); в данном режиме терминалы Globalstar должны в среднем потреблять энергии меньше, чем аналоговые сотовые телефоны, и, соответственно, продолжительность работы их аккумуляторов должна быть больше.

Мобильные терминалы отличаются от портативных дополнительным усилителем мощности и внешней антенной. Мощность мобильного терминала не превышает 3 Вт.

Стационарные аппараты Globalstar предоставят услуги связи в отдаленных районах, где нет ни сотовых систем, ни наземных коммуникаций. Такие терминалы предназначены для работы только в ССПС Globalstar. Они оборудованы усилителем и внешней антенной с усилением +7дБ и имеют эквивалентную изотропно-излучаемую мощность 3,2 Вт.

Компания Globalstar намерена предлагать услуги связи по более низким тарифам, чем те, что используются в настоящее время в системе Iridium. Предусматривается дифференцирование цен в зависимости от географического района и уровня сервисных услуг: 0,35; 0,53; 1; 3 долл. за 1 мин разговора. В среднем стоимость одноминутного соединения должна находиться в пределах 0,35-0,65 долл. США плюс плата за услуги местных (наземных) линий связи. Ожидаемая цена портативного терминального устройства производства фирмы QUALCOMM также гораздо меньше, чем спутникового телефона системы Iridium, и

составляет около 700 долл.. Компания Globalstar L.P. считает, что принятая ею структура ценообразования будет способствовать более быстрому распространению услуг и позволит ей создать широкий круг постоянных клиентов. Ожидается, что к 2002 году число абонентов ССПС Globalstar превысит 2,7 млн., а к 2012 году, по мнению разработчиков проекта, система сможет обслужить до 14 млн. пользователей.

Есть основания предполагать, что после ввода в строй системы Globalstar и устранения монопольного положения на рынке услуг спутниковой персональной связи ССПС Iridium цены на услуги и оборудование последней будут в значительной степени снижены.

Предполагается использование системы Globalstar и на российском рынке, так как он становится все более открытым для зарубежных поставщиков услуг. Кроме того, в России требования пользователей к уровню услуг в последнее время возросли, и появились потребители, способные оплачивать услуги ССПС. Планируемый рынок Globalstar в России составляет примерно 7,5 % от мирового. Проект российского сегмента ССПС Globalstar разработан институ-

том “Гипросвязь” по заказу “АО Ростелеком”. В соответствии с данным проектом в настоящее время на территории России уже строятся 3 станции сопряжения (в Москве, Новосибирске и Хабаровске), а к 2005 году предполагается соорудить 9 станций сопряжения, способных обслуживать 260 тыс. пользователей. Национальным оператором и эксклюзивным поставщиком услуг системы Globalstar в России является ЗАО “ГлобалТел”, которое учреждено компанией Globalstar Ltd. и “АО Ростелеком” в 1996 году.

В настоящее время консорциум Globalstar имеет соглашения с провайдером услуг более чем в 100 странах. Первые 8 космических аппаратов были выведены на орбиту Земли еще в начале 1998 года с использованием ракет-носителей (РН) Delta II, но 9 сентября 1998 года попытка запуска 12 космических аппаратов Globalstar с помощью РН “Зенит” потерпела неудачу...

После 2004 года, когда система работает свой ресурс, компания Globalstar планирует замену существующей аппаратуры первого поколения на усовершенствованную аппаратуру системы Globalstar-II.

## **Ретрансляторы**

Радиотелефоны представляют собой радиостанции малой мощности. Владелец такого устройства связывается с еще одной радиостанцией, представляющей вторую часть данной индивидуальной системы связи, которая обычным образом подключена к телефонной линии. Используя эти две радиостанции пользователь получает возможность дуплексной связи как по обычному телефону, конечно, в пределах дальности связи, определяемой мощностью данных устройств. Для индивидуальных радиотелефонов, подключаемых самим пользователем к телефону (второй части системы, часто называемой базой), дальность может достигать 1-2 км. Как правило, такие радиотелефоны работают на частоте 900 МГц.

Ниже будут представлены и описаны устройства, подключаемые к телефонной линии и предоставляющие возможность прослушивать телефонные разговоры по АМ- или ЧМ-радиоприемникам. Это позволяет, например, обеспечить громкое прослушивание, записывать разговор на магнитофон магнитолы (непосредственно или через соответствующий конвертер). Такие радиоприемники, подключаемые к телефону

ной линии, называются телефонными ретрансляторами. В зависимости от типа используемой модуляции эти устройства разделяются на АМ- и ЧМ-ретрансляторы.

Данные ретрансляторы представляют собой однотранзисторные АМ-передатчики, выполненные на основе традиционных схем ВЧ-генераторов на биполярных транзисторах. Эти схемы часто встречаются в описании предыдущих устройств. Передающей антенной, излучающей радиоволны, для данных устройств служит один из проводников (одна жила) телефонного провода. Эти телефонные АМ-ретрансляторы обеспечивают дальность передачи на несколько десятков метров. Данные АМ-ретрансляторы устанавливаются внутрь телефонного аппарата. Подключение выполняется параллельно микрофону и телефону.

Необходимо соблюдать полярность подключения.

Монтаж выполняется на 2-стороннем фольгированном стеклотекстолите. Одна сторона (со стороны деталей) используется как общий провод и экран, другая - для печатных проводников схемы. Проводники, соединяющие детали, должны иметь минимальную длину. Для повышения стабильно-

сти частоты целесообразно поместить задающий генератор или все устройство в экран.

Используя ранее приведенные и описанные схемы задающих генераторов на МОП-транзисторах можно создать простые и компактные телефонные АМ-ретрансляторы. Данные устройства предназначены для работы на частоте 27 МГц, но, как и предыдущие варианты АМ-ретрансляторов, эти схемы могут использоваться и в других частотных диапазонах - на более низких и более высоких частотах. Дальность - несколько десятков метров.

Монтаж выполняется на 2-стороннем фольгированном стеклотекстолите. Одна сторона (со стороны деталей) используется как общий провод и экран, другая - для печатных проводников схемы. Проводники, соединяющие детали, должны иметь минимальную длину. Для повышения стабильности частоты целесообразно поместить задающий генератор или все устройство в экран. Передающей антенной служит один из проводников телефонного провода.

Мощность (и дальность) телефонных АМ-ретрансляторов может быть увеличена за счет введения в схему дополнительных

ВЧ-каскадов - усилителей мощности. В качестве примера таких дополнительных каскадов можно использовать ранее описанные схемы АМ- и ЧМ-радиопередатчиков повышенной мощности.

Используя схемы УКВ ЧМ-передатчиков на биполярных и МОП-транзисторах можно создать простые телефонные УКВ ЧМ-ретрансляторы. Данные схемы имеют сходные элементы, особенности конструкции и настройки с УКВ ЧМ-радиопередатчиками.

Монтаж выполняется на 2-стороннем фольгированном стеклотекстолите. Одна сторона (со стороны деталей) используется как общий провод и экран, другая - для печатных проводников схемы. Проводники, соединяющие детали, должны иметь минимальную длину. Для повышения стабильности частоты целесообразно поместить задающий генератор или все устройство в экран. При этом частота генератора, возможно, несколько изменится (увеличится).

## **Взлом**

### **Мобильная связь**

В России функционируют федеральные сети стандартов GSM 900/1800 и NMT-450, а также региональные сети AMPS/DAMPS. На 1 января 2001 г. эти сети охватывали 74 региона России, предоставляя услуги 1,925 млн. абонентов. В итоге, показатель проникновения (отношение количества мобильных абонентов в общему количеству населения страны) составляет 0,7%. Характерной особенностью мобильной связи в России является значительная концентрация абонентов в Московском и Ленинградском регионах, где их численность достигает 73% от общего числа российских абонентов, с показателем проникновения 3%.

На остальной территории России без учета двух упомянутых регионов проникновение мобильной связи оказывается менее 0,2%. Половина всех операторов обслуживает на своей территории менее 1000 абонентов.

Частотный ресурс является самым ценным в мобильной связи и Россия наконец-то отнесена к европейским государствам — с соответствующим распределением частот. Это означает, что для высвобождения необходимых полос частот для сетей GSM будут выводиться из эксплуатации устаревшие радиоэлектронные средства фиксированной службы правительственного и гражданского назначения, работающие в этом частотном диапазоне. Для ускорения этого процесса заинтересованные операторы могут переводить эти средства в другие диапазоны, к примеру 2025 — 2110 МГц.

Согласно проекту «Концепции программы развития связи и информатизации Российской Федерации до 2015 г.», предполагается, что количество абонентов мобильной связи к 2010 г. достигнет 15 млн. (показатель проникновения 9,3%).

Дальнейшее развитие мобильной связи в России должно происходить в русле существующих мировых тенденций, связанных прежде всего с внедрением технологий подвижной связи 3-го поколения.

Поскольку внедрение систем 3-го поколения начнется с небольшого числа крупных городов, в которых могут быть востре-

бованы в приемлемом объеме современные услуги, «зонтичное» покрытие территории в масштабах лицензируемого региона, страны и всего земного шара может быть осуществлено только при взаимодействии с существующими сетями 2-го поколения. Техническая возможность такого взаимодействия заложена оборудованием систем 3-го поколения в виде так называемой «обратной совместимости».

Существующие в России сети трех стандартов целесообразно развивать следующим образом. Аналоговые сети стандарта NMT-450 с целью повышения их инвестиционной привлекательности и исходя из геополитических интересов России модернизируются на базе технологии GSM. При этом сети стандарта NMT-450 должны продолжать обслуживание собственных абонентов и предоставлять услуги роуминга течение срока действия нынешних NMT-лицензий, а при наличии экономической целесообразности и в течение более длительного срока.

Аналого-цифровые сети стандарта AMPS/DAMPS после завершения перевода на цифровой вариант (в версии TDMA IS-136) могут эволюционировать к 3-му поко-

лению в диапазоне 800 МГц поэтапно с использованием технологии радиоинтерфейса IMT-SC, завершающейся введением версии стандарта EDGE (Enhanced Data Rates for the GSM Evolution).

Сети стандарта GSM должны эволюционировать к 3-му поколению в соответствии с последними версиями стандартов ETSI. На первом этапе может быть использована технология HSCSD (High Speed Circuit Switched Data), обеспечивающая скорости передачи данных до 57,6 Кбит/с в режиме с коммутацией каналов. Более радикальный способ увеличения пропускной способности состоит в использовании технологии GPRS (General Packet Radio Service), основанной на режиме коммутации пакетов при передаче со скоростью 115 Кбит/с. Этот режим обеспечит «постоянное» подключение абонентов к сети с взиманием платы только за объем переданных данных. В качестве последнего шага на пути эволюционного перехода к 3-му поколению следует использовать технологию EDGE, обеспечивающую передачу данных со скоростями до 384 Кбит/с с реализацией полного набора услуг 3-го поколения.



## **GSM**

GSM является цифровой сотовой связью с рабочей частотой 900 МГц. По воздуху сигнал передается в цифровом формате, за счет этого сохраняется высокое качество связи. Средний GSM-аппарат без вспомогательного оборудования может работать на расстоянии до 1500 метров от станции.

Большое распространение система GSM получила во многих странах Европы. Постепенно распространяется и на других континентах.

## **SIM карточки**

SIM (Subscriber Identity Module) карта представляет собой чип, в который «прошит» определенный абонентный номер. В SIM карте имеется память для записной книжки, рассчитанная на 100 или более номеров. Для защитных функций SIM карте присваиваются коды PIN (Personal Identification Number) и PUK (Personal Unlocked Key). Код PIN нужно вводить при включении аппарата, таким образом человек, не знающий его, включить аппарат не сможет.

Можно выключить запрос кода PIN, а также этот код можно поменять. Это делается с помощью меню телефона или командой:

### **04 старый PIN новый PIN новый PIN**

В случае, если код PIN был неправильно набран 3 раза, карта блокируется и запрашивает PUK код, который состоит из 8 цифр. Для того, чтобы разблокировать карту нужно ввести команду:

05 PUK новый PIN новый PIN

В случае, если код PUK был введен неправильно 10 раз и вся информация с карточки была стерта, или PUK код был утерян, нужно обращаться к своему оператору сети. В память карты также записаны код PIN2 и для его изменения PUK2. Изменение PIN2 осуществляется с помощью команды:

042 старый PIN2 новый PIN2 новый PIN2  
или

052 PUK2 новый PIN2 новый PIN2

Код PIN2 используется при сбрасывании счетчиков разговора, при вкл/выкл запрета вызовов — это зависит от модели телефона.

### Станции GSM

Площадь, охватываемая сетью GSM, разбита на ячейки, посреди которых находятся передающие станции. Обычно станция имеет шесть передатчиков, которые расположены с диаграммой направленности 120 градусов и равномерно покрывают площадь. Одна средняя станция одновременно может обслуживать до 80 каналов. Зона покрытия соседних станций соприкасается. При передвижении телефонного аппарата между станциями, происходит его регистрация.

В пригородах и районах для размещения передатчиков используются вышки в несколько секций. Их часто можно увидеть расположенными вдоль шоссе. А также кое-где в городах, где нет достаточно высоких домов.

В городах, где есть достаточно высокие дома, передатчики расположены прямо на крышах домов. В таких случаях количество передатчиков может меняться в зависимости от внешних факторов.

### CMG

Система CMG вводится в действие на системе «Белсел» (Белоруссия, NMT450).

Предназначена для защиты информации на сотовой сети, будет соединена с базой данных более 30.000 абонентов «Белсел». Сопряжение «Белсел» с «Сотел» организует ЗАО «Межрегионтранзиттелеком».

### FraudBuster

**FraudBuster** — система обнаружения фрода и формирования профиля абонента, предназначена для обнаружения и борьбы, в том числе и с новыми видами фрода. Система, выбранная на 99.01 уже 27 сотовыми компаниями в мире, способна накапливать данные о вызовах каждого конкретного абонента и создавать на этой основе индивидуальные профили каждого абонента. Они затем дополняются, анализируются по мере совершения новых звонков и способны немедленно обнаруживать аномальную активность, которая может свидетельствовать о факте фрода. Поскольку инфраструктура не связана с концепцией системы защиты, то она подходит для систем GSM, AMPS, CDMA, TDMA и iDEN.

Несмотря на повсеместное внедрение систем защиты сотовой связи от фрода — проблема несанкционированного подключения и воровства эфирного времени в со-

товых системах, к примеру, в США стоит весьма серьезно. Ожидается, к примеру, что в 2002 году потери от фрода составят 677 млн.\$, в то время как в 1998 году они составили 540 млн.\$.

Клонирование, согласно исследованию, уже не является значимым фактором, так как с ним научились эффективно бороться. В качестве превентивных мер предлагается использование PIN, RF-отпечатков (fingerprints), аутентификацию, проверки баз данных абонентов, систем с предоплатой, систем безопасности и биллинга в реальном времени. По-видимому, даже появление новых систем защиты не позволит полностью решить проблему защиты от фрода, так что сотовым операторам нужно следить за появлением все новых способов фрода и своевременно предпринимать соответствующие защитные меры.

Предоплаченный сервис, который так усердно внедряется во всем мире, по мнению экспертов может стать основным источником проблем с фродом в ближайшем будущем. Есть мнение, что уже сейчас операторы столкнулись с фродом, теряя столько же денег, сколько и при традиционной системе контрактов. Предоплаченный сер-

вис воспринимался как панацея от неплатежей и традиционного фрода, особенно его ранняя версия, когда услуги продавались по принципу «используй-или-пропадет» — то есть нужно было воспользоваться предоплаченными минутами в определенный период времени. В то же время, это привлекало прежде всего тех, кто мог иметь проблемы с кредитной историей, или не хотел платить абонентской платы, собираясь использовать телефон лишь в каких-то редких ситуациях, и в то же время был готов платить больше за минуту разговора в экстренной ситуации.

Сегодня предоплаченную карточку можно свободно купить и именно такие аккаунты открыты 40% новых мобильных абонентов по всему миру. В качестве уязвимых с точки зрения фрода, специалисты отметили — Smart карты, основанные на SIM (Subscriber Identification Modules), в которые могут быть внесены изменения; система ваучеров, использующаяся для покупки времени, которая может быть нарушена при печати или при продаже. И, как обычно, предоплата может осуществляться краденными или поддельными чеками, кредитками или банковскими картами.

## **Ловушки**

Для того, чтобы лучше понять проблемы, связанные с использованием беспроводных средств связи, давайте вспомним, что эти средства из себя представляют и как работают.

Современные беспроводные средства персональной связи включают в себя мобильные телефоны сотовой связи, пейджеры и беспроводные стационарные радиотелефоны.

### **Сотовые телефоны**

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. Каждому сотовому телефонному аппарату присваивается свой электронный серийный номер (ESN), который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот номер в руководстве для пользователя. При подключении аппарата к сотовой системе связи, техники компании, предоставляющей услуги этой связи, дополнительно заносят в микрочип телефона еще

и мобильный идентификационный номер (MIN). Мобильный сотовый телефон имеет большую, а иногда и неограниченную дальность действия, которую обеспечивает сотовая структура зон связи. Вся территория, обслуживаемая сотовой системой связи, разделена на отдельные, прилегающие друг к другу, зоны связи или «соты».

Телефонный обмен в каждой такой зоне управляется базовой станцией, способной принимать и передавать сигналы на большом количестве радиочастот. Кроме того, эта станция подключена к обычной проводной телефонной сети и оснащена аппаратурой преобразования высокочастотного сигнала сотового телефона в низкочастотный сигнал проводного телефона и наоборот, чем обеспечивается сопряжение обеих систем.

Периодически (с интервалом 30-60 минут) базовая станция излучает служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои MIN- и ESN-номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и

привязка аппарата к определенной зоне, в которой он находится в данный момент времени. Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению. В случае, если мобильный пользователь во время разговора перемещается из одной зоны связи в другую, базовая станция покидаемой зоны автоматически переводит сигнал на свободную частоту новой зоны.

### **Пейджеры**

Пейджеры представляют собой мобильные радиоприемники с устройством регистрации сообщений в буквенном, цифровом или смешанном представлении, работающие, в основном, в диапазоне 100-400 МГц. Система пейджинговой связи принимает сообщение от телефонного абонента, кодирует его в нужный формат и передает на пейджер вызываемого абонента.

### **Беспроводные радиотелефоны**

Стационарный беспроводный радиотелефон объединяет в себе обычный проводной телефон, представленный самим

аппаратом, подключенным к телефонной сети, и приемопередающее радиоустройство в виде телефонной трубки, обеспечивающей двусторонний обмен сигналами с базовым аппаратом. В зависимости от типа радиотелефона, дальность связи между трубкой и аппаратом, с учетом наличия помех и переотражающих поверхностей, составляет в среднем до 50 метров.

Проблема безопасности при использовании сотовым телефоном и другими мобильными средствами персональной беспроводной связи имеет два аспекта: физическая безопасность пользователя и безопасность информации, передаваемой с помощью этих устройств. Здесь сразу следует оговориться, что угрозу физической безопасности создает только мобильный сотовый телефон, так как пейджеры и стационарные радиотелефоны являются неизлучающими или слабо излучающими устройствами и характеризуются отличными от сотовых телефонов условиями и порядком пользования.

Вы, наверное, не раз слышали рекламу компаний, предоставляющих услуги сотовой связи: «Надежная связь по доступной цене!». Давайте проанализируем, действи-

тельно ли она так уж надежна. С технической точки зрения — да. А с точки зрения безопасности передаваемой информации?

В настоящее время электронный перехват разговоров, ведущихся по сотовому или беспроводному радиотелефону, стал широко распространенным явлением.

Так, к примеру, в Канаде, по статистическим данным, от 20 до 80% радиообмена, ведущегося с помощью сотовых телефонов, случайно или преднамеренно прослушивается посторонними лицами.

Электронный перехват сотовой связи не только легко осуществить, он, к тому же, не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. На Западе прослушивание и/или запись разговоров, ведущихся с помощью беспроводных средств связи, практикуют правоохранные органы, частные детективы, промышленные шпионы, представители прессы, телефонные компании, компьютерные хакеры.

В западных странах уже давно известно, что мобильные сотовые телефоны, особенно аналоговые, являются самыми уязвимыми с точки зрения защиты передаваемой

информации.

Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое ваше слово. Для этого даже не нужно иметь особо сложной аппаратуры. Разговор, ведущийся с сотового телефона, может быть прослушан с помощью продающихся на Западе программируемых сканеров с полосой приема 30 кГц, способных осуществлять поиск в диапазоне 860–890 МГц. Для этой же цели можно использовать и обычные сканеры, после их небольшой модификации, которая, кстати, весьма подробно описана в Internet. Перехватить разговор можно даже путем медленной перестройки УКВ-тюнера в телевизорах старых моделей в верхней полосе телевизионных каналов (от 67 до 69), а иногда и с помощью обычного радиотюнера. Наконец, такой перехват можно осуществить с помощью ПК.

Легче всего перехватываются неподвижные или стационарные сотовые телефоны, труднее — мобильные, так как перемещение абонента в процессе разговора со-

проводится снижением мощности сигнала и переходом на другие частоты в случае передачи сигнала с одной базовой станции на другую.

Более совершенны с точки зрения защиты информации цифровые сотовые телефоны, передающие информацию в виде цифрового кода. Однако, используемый в них алгоритм шифрования Cellular Message Encryption Algorithm (CMEA) может быть вскрыт опытным специалистом в течение нескольких минут с помощью персонального компьютера. Что касается цифровых кодов, набираемых на клавиатуре цифрового сотового телефона (телефонные номера, номера кредитных карточек или персональные идентификационные номера PIN), то они могут быть легко перехвачены с помощью того же цифрового сканера.

Не менее уязвимыми с точки зрения безопасности информации являются беспроводные радиотелефоны. Они при работе используют две радиочастоты: одну — для передачи сигнала от аппарата к трубке (на ней прослушиваются оба абонента), другую — от трубки к аппарату (на ней прослушивается только абонент, говорящий в эту трубку). Наличие двух частот еще больше

расширяет возможности для перехвата.

Перехват радиотелефона можно осуществить с помощью другого радиотелефона, работающего на тех же частотах, радиоприемника или сканера, работающих в диапазоне 46-50 МГц. Дальность перехвата, в зависимости от конкретных условий, составляет в среднем до 400 метров, а при использовании дополнительной дипольной антенны диапазона 46-49 МГц — до 1,5 км.

Следует отметить, что такие часто рекламируемые возможности беспроводного телефона, как «цифровой код безопасности» (digital security code) и «снижение уровня помех» (interference reduction), нисколько не предотвращают возможность перехвата разговоров. Они только препятствуют несанкционированному использованию этого телефона и не дают соседствующим радиотелефонам звонить одновременно. Сложнее перехватить цифровые радиотелефоны, которые могут использовать при работе от 10 до 30 частот с автоматической их сменой. Однако и их перехват не представляет особой трудности при наличии радиосканера.

Таковыми же уязвимыми в отношении безопасности передаваемой информации являются и пейджеры. В большинстве сво-

ем они используют протокол POSCAG, который практически не обеспечивает защиты от перехвата. Сообщения в пейджинговой системе связи могут перехватываться радиоприемниками или сканерами, оборудованными устройствами, способными декодировать коды ASCII, Baudot, CTCSS, POCSAG и GOLAY. Существует также целый ряд программных средств, которые позволяют ПК в сочетании со сканером автоматически захватывать рабочую частоту нужного пейджера или контролировать весь обмен в конкретном канале пейджинговой связи. Эти программы предусматривают возможность перехвата до 5000 пейджеров одновременно и хранение всей переданной на них информации.

## **Клонирование**

Мошенничество в сотовых системах связи, известное еще под названием «клонирование», основано на том, что абонент использует чужой идентификационный номер (а, следовательно, и счет) в корыстных интересах. В связи с развитием быстродействующих цифровых сотовых технологий, способы мошенничества становятся все более изощренными, но общая схема их тако-

ва: мошенники перехватывают с помощью сканеров идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции, выделяют из него идентификационные номера MIN и ESN и перепрограммируют этими номерами микрочип своего телефона. В результате, стоимость разговора с этого аппарата заносится базовой станцией на счет того абонента, у которого эти номера были украдены.

Например, в больших городах Запада, чаще всего в аэропортах, работают мошенники, которые, клонировав ESN-номер чьего-либо мобильного телефона, предлагают за плату возможность другим людям звонить с этого телефона в отдаленные страны за счет того, чей номер выкрали.

Кража номеров осуществляется, как правило, в деловых районах и в местах скопления большого количества людей: шоссе, дорожные пробки, парки, аэропорты, — с помощью очень легкого, малогабаритного, автоматического оборудования. Выбрав удобное место и включив свою аппаратуру, мошенник может за короткий промежуток времени наполнить память своего устройства большим количеством номеров.



Наиболее опасным устройством является так называемый сотовый кэш-бокс, представляющий собой комбинацию сканера, компьютера и сотового телефона. Он легко выявляет и запоминает номера MIN и ESN и автоматически перепрограммирует себя на них. Используя пару MIN/ESN один раз, он стирает ее из памяти и выбирает другую. Такой аппарат делает выявление мошенничества практически невозможным. Несмотря на то, что эта аппаратура на Западе пока еще редка и дорога, она уже существует и представляет растущую опасность для пользователей сотовой связи.

## **Выявление местоположения абонента**

Оставим в стороне такую очевидную возможность, как выявление адреса абонента сотовой системы связи через компанию, предоставляющую ему эти услуги. Немногие знают, что наличие мобильного сотового телефона позволяет определить как текущее местоположение его владельца, так и проследить его перемещения в прошлом.

Текущее положение может выявляться двумя способами. Первым из них является обычный метод триангуляции (пелен-

гования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура хорошо разработана, обладает высокой точностью и вполне доступна.

Второй метод — через компьютер предоставляющей связь компании, который постоянно регистрирует, где находится тот или иной абонент в данный момент времени даже в том случае, когда он не ведет никаких разговоров (по идентифицирующим служебным сигналам, автоматически передаваемым телефоном на базовую станцию, о которых мы говорили выше). Точность определения местонахождения абонента в этом случае зависит от целого ряда факторов: топографии местности, наличия помех и переотражений от зданий, положения базовых станций, количества работающих в настоящий момент телефонов в данной соте. Большое значение имеет и размер соты, в которой находится абонент, поэтому точность определения его положения в городе гораздо выше, чем в сельской местности (размер соты в городе составляет около 1 кв. км против 50-70 кв. км на открытой местности) и, по имеющимся данным, составля-

ет несколько сот метров.

Наконец, анализ данных о сеансах связи абонента с различными базовыми станциями (через какую и на какую базовую станцию передавался вызов, дата вызова) позволяет восстановить все перемещения абонента в прошлом. Такие данные автоматически регистрируются в компьютерах компаний, предоставляющих услуги сотовой связи, поскольку оплата этих услуг основана на длительности использования системы связи. В зависимости от фирмы, услугами которой пользуется абонент, эти данные могут храниться от 60 дней до 7 лет.

Такой метод восстановления картины перемещений абонента очень широко применяется полицией многих западных стран при расследованиях, поскольку дает возможность восстановить с точностью до минут, где был подозреваемый, с кем встречался (если у второго тоже был сотовый телефон), где и как долго происходила встреча или был ли подозреваемый поблизости от места преступления в момент его совершения.

### **Некоторые советы**

Проблема безопасности при использовании современных беспроводных средств связи достаточно серьезна, но, используя здравый смысл и известные приемы противодействия, ее можно, в той или иной степени, решить. Не будем затрагивать тех мер, которые могут предпринять только провайдеры связи (к примеру, введение цифровых систем). Поговорим о том, что можете сделать вы сами.

Для предотвращения перехвата информации:

**Используйте общепринятые меры по предупреждению раскрытия информации:** избегайте или сведите к минимуму передачу конфиденциальной информации, такой как номера кредитных карточек, финансовые вопросы, пароли. Прибегайте в этих целях к более надежным проводным телефонам, убедившись, однако, что ваш собеседник не использует в этот момент радиотелефон. Не используйте сотовые или беспроводные телефоны для ведения деловых разговоров.

**Помните, что труднее перехватить разговор, который ведется с движущегося автомобиля,** так как расстояние между ним и перехватывающей аппаратурой (если та нахо-

дится не в автомобиле) увеличивается и сигнал ослабевает. Кроме того, при этом ваш сигнал переводится с одной базовой станции на другую с одновременной сменой рабочей частоты, что не позволяет перехватить весь разговор целиком, поскольку для нахождения этой новой частоты требуется время.

**Используйте системы связи, в которых данные передаются с большой скоростью** при частой автоматической смене частот в течение разговора.

**Используйте, при возможности, цифровые сотовые телефоны.**

**Отключите полностью свой сотовый телефон**, если не хотите, чтобы ваше местоположение стало кому-то известно.

В случае использования беспроводного радиотелефона:

- при покупке выясните, какую защиту он предусматривает.
- используйте радиотелефоны с автоматической сменой рабочих частот типа «spread spectrum» или цифровые, работающие на частотах порядка 900 МГц.

- по возможности, используйте радиотелефоны со встроенным чипом для шифрования сигнала.

Для предотвращения мошенничества:

- узнайте у фирмы-производителя, какие средства против мошенничества интегрированы в ваш аппарат.
- держите документы с ESN-номером вашего телефона в надежном месте.
- ежемесячно и тщательно проверяйте счета на пользование сотовой связью.
- в случае кражи или пропажи вашего сотового телефона сразу предупредите фирму, предоставляющую вам услуги сотовой связи.
- держите телефон отключенным до того момента, пока вы не решили им воспользоваться. Этот способ самый легкий и дешевый, но следует помнить, что для опытного специалиста достаточно одного вашего выхода на связь, чтобы выявить MIN/ESN номера вашего аппарата.
- регулярно меняйте через компанию, предоставляющую вам услуги сотовой связи, MIN-номер вашего аппарата.

Этот способ несколько сложнее предыдущего и требует времени.

- попросите компанию, предоставляющую вам услуги сотовой связи, установить для вашего телефона дополнительный 4-х значный PIN-код, набираемый перед разговором. Этот код затрудняет деятельность мошенников, так как они обычно перехватывают только MIN и ESN номера, но, к сожалению, небольшая модификация аппаратуры перехвата позволяет выявить и его.
- наиболее эффективным методом противодействия является шифрование MIN/ESN номера (вместе с голосовым сигналом) по случайному закону.

## Шифрование

Два выдающихся израильских фрикера повергли в шок специалистов по защите информации, заявив, что они нашли способ извлечь криптографические ключи DES из ПК и смарт-карт. Ади Шамир, один из трех авторов разработки методологии шифрования с открытыми ключами, и Эли Бихам утверждают, что они могут получить даже

168-разрядный секретный ключ Triple-DES. Криптографы использовали нагревание или излучение для изменения битовой последовательности ключа. Затем, применив методику под названием Differential Fault Analysis (DFA), они сравнивали зашифрованный вывод с поврежденной и неповрежденной картой для поиска ключа.

56-разрядный стандарт DES одобрен правительством США для использования в банковской сфере и широко реализован в программных и аппаратных продуктах.

Эксперты по защите информации считают, что открытие Шамира и Бихама поставило под сомнение возможность использования смарт-карт с шифрованием, в особенности для электронных расчетов. Получив криптографический ключ, мошенники могут снять всю наличность с карты. Эксперты добавляют также, что организации, использующие DES, с целью предотвращения DFA-атак должны будут закрыть посторонним физический доступ к устройствам шифрования DES.

При помощи аналогичного метода ученые из Bellcore взломали защиту смарт-карты с шифрованием по методу открытых ключей RSA. Такая технология взлома,

вполне вероятно, вскоре пополнит арсенал фрикеров.

Смарт-карты с микропроцессорами для хранения персональных данных и электронной наличности весьма популярны, особенно в Европе. Вильям Каелли, профессор Квинсландского технологического университета, полагает, что к 2000 году будет использоваться свыше 300 млн. карт.

Каелли утверждает, что некоторые изготовители карт, к примеру Siemens GmbH, подходят к производству этого продукта очень ответственно. Однако на рынке большинство карт настолько плохи, что мошенники со считывателем смарт-карт ценой 180 долларов и компьютером могут без труда записать процесс шифрования.

Стив Велловин, ученый из AT&T Laboratories, считает, что открытие Bellcore и Шамира-Бихама будет иметь серьезные последствия для разработок в области смарт-карт и электронной наличности.

Белловин добавляет, что в конечном счете это открытие позволяет нам лучше понять уязвимые места устройств шифрования данных, используемых в банках и других организациях для передачи больших

объемов информации.

Оборудование нужно постоянно проверять на наличие слабых мест. Например, 40-разрядный ключ может быть легко найден при помощи так называемого метода грубой силы, то есть прямого перебора на компьютере в поисках ключа.

В свое время Netscape communications подверглась публичному унижению — студенты из Беркли без труда взломали систему шифрования Navigator. Это стало возможным из-за неудачного выбора генератора случайных чисел. Netscape немедленно исправила выявленный недостаток.

Одна компания — Access Data — зарабатывает себе на жизнь тем, что взламывает системы шифрования по заказу следственных органов и корпораций.

По словам президента Access Data Эрика Томпсона, его компания взломала 90% систем шифрования в проверяемых ею коммерческих программах шифрования от Microsoft, Borland International и IBM, в частности посредством атаки на используемые программами системы паролей.

## Пейджеры

Чтение пейджерных сообщений практически любой российской пейджерной компании с применением компьютера не составляет никакого труда. Также легко осуществляется и передача на любой пейджер. Но вы должны знать — *любое* использование полученной таким образом информации против третьих лиц является преступлением. Вы должны использовать информацию этой главы *только* для радиолюбительских целей! За рубежом радиолюбительский пейджинг является очень популярным увлечением. Многие радиолюбители на своих сайтах предлагают рекристаллинг (замену кварцевого резонатора) для перестройки пейджера на любительский диапазон. Стоит это у них порядка 20 долларов с пересылкой по почте. О сколько-нибудь серьезном развитии любительского пейджинга в России пока ничего не известно.

Вам потребуется:

- Компьютер, имеющий саундбластер или свободный СОМ-порт. Для передачи наличие СОМ-порта обязательно.

- УКВ-радиостанция. Большинство пейджинговых компаний России работают в диапазоне около 160 МГц (к примеру, 159,020 МГц и 159,050 МГц). Идеально подойдет «незащищенный» Kenwood, Motorola, Alinco или аналогичный аппарат. Можно, конечно, и самодельный.
- Собственно программа. Рекомендована — РОС32.

Программа прекрасно работает на прием со всеми звуковыми картами, обеспечивающими качественную запись звука. Но для устойчивого декодирования обязательно надо подключать линейный вход саундкарты непосредственно к выходу дискриминатора приемника. При прохождении через УНЧ, фронты сигнала значительно искажаются и читаемость сообщений всего 7-8%, а с дискриминатора — 99-100% при тех же условиях приема.

Программа потребует настройки кодовой таблицы (их может быть несколько). Начальная таблица имеет имя **Default.tbl**. Сделайте ее копию и начинайте настраивать.

Запустите программу на прием сообщений. Во встроенном блокноте **Windows Notepad** откройте ваш файл кодовой таблицы. Столбец слева — принимаемый код, справа — его отображение на экране. Посмотрите на принимаемых сообщениях, какие буквы нужно исправлять и замените их в кодовой таблице. Сохраните файл и переустановите его в меню **Properties**. При необходимости повторите процесс.

Проблема в том, что даже в одной пейджинговой компании могут быть пейджеры разных типов, с разными кодировками. Например, с транслитерацией, когда русские слова пишут латинскими буквами. Они различаются диапазоном номеров либо номером функции. Одновременно правильно декодировать сообщения для разных систем не получится, так как действует только одна таблица кодов, не переключаемая динамически. Этот недостаток программы, вероятно, будет вскоре исправлен.

### Взлом пейджеров

Пейджерные системы на территории бывшего СССР в основном работают в протоколе POCSAG. Этот протокол стандартизован CCIR (теперь ITU).

Техническая спецификация на протокол POCSAG содержится в соответствующей рекомендации ITU (R.584-1). Эту рекомендацию на русском языке можно найти, к примеру, в ГПТБ. Существуют и «самодельные» описания протокола POCSAG: к примеру, в комплекте пейджерного декодера PD 2.xx содержится текстовый файл с кратким описанием протокола.

Для того, чтобы просканировать пейджинговую систему, нужно изготовить так называемый сканер POCSAG.

Для этого нужно взять NFM-приемник на частоту нужной компании-провайдера, к примеру 160.0375 для RadioPage, выход с детектора приемника пропустить через компаратор для преобразования в логические уровни RS-232, а цифровой выход с компаратора подать на 5 и 6 пин 25-пинового разъема RS-232. Разъем присоединить к COM-порту компьютера и запустить соответствующую программу, принимающую и декодирующую пейджерные сообщения.

На свете для этих дел существуют программы-декодеры POCSAG:

- **PageMaster** (поддержка русских кодировок, фильтры, удобный интерфейс,

но не очень хороший приемник).

- **Prizma-1** (поддержка русских кодировок, хороший цифровой декодер, фильтры, интерфейс крайне корявый).
- **Prizma-8** (тоже, что Prizma-1, но декодирует одновременно 8 каналов).
- **PD 2.xx** (буржуйский декодер, нет поддержки русских кодировок, интерфейса нет вообще).

Для того, чтобы сделать двойника на пейджер нужно определить капкод пейджера по его номеру и зашить полученный капкод с помощью программатора во второй пейджер.

## Секретные коды

Описанные ниже манипуляции гарантированно подходят для сотовых телефонов Ericsson DH336, DH338, DH343, DH353, а также DF388. Скорее всего, подойдут и для других модификаций Ericsson, но это уже надо пробовать.

В память упомянутых телефонов могут быть записаны четыре набора данных, включающих в себя городской номер и па-

роль для его изменения, идентификатор системы и некоторые другие параметры для систем, поддерживающих услуги пейджинга и голосовой почты. Переключаться между этими наборами установок можно из обычного меню, если вам известен пароль. По умолчанию это четыре нуля. Для чего это нужно? Например, вы можете с одним аппаратом быть официально прописаны в четырех разных городах у четырех разных провайдеров. Приехав в другой город, вы включаете соответствующий городской номер и тарифицируетесь именно у данного провайдера. Это не автоматический роуминг, а именно переключение вручную. У каждой сотовой системы в каждом городе свой идентификационный номер.

Таким образом, зная служебные коды трубки, вы можете изменить прописанный в ней городской номер, изменить номер сотовой системы, записать три дополнительных городских номера, изменить или установить пароли для их защиты.

К сожалению, таким способом вы не сможете создать полный двойник трубки. Дело в том, что во флэш-память каждой трубки на заводе зашивают ее личный **Equipment Serial Number (ESN#)** из 11 зна-



ков. Он цифрами и штрих-кодом записан на задней стенке трубки. Изменить этот номер можно только программированием с помощью специального программатора. Схемы программатора и разводка выводов трубок известны, а программу, как таковую, найти пока не удалось. Зарубежные фрике-ры как-то ловко умалчивают этот вопрос, а отечественные утверждают, что перепрограммирование ESN# невозможно, по крайней мере для последних моделей, и трубу можно просто убить. Этот вопрос еще надо уточнить.

При активизации трубки у провайде-ра, ее ESN# записывается в память систем-ного компьютера и при установлении связи проверяется соответствие ESN# и городско-го номера. При несовпадении, трубка от си-стемы отключается.

Однако и на этом уровне можно де-лать интересные вещи. Програмируем в трубку городской номер чьей-нибудь труб-ки из этой же системы. При входящем звон-ке на этот номер если:

- вы находитесь в зонах действия раз-ных сот, ваши две трубки подтверж-дают прием звонка одновременно с разных сот (это делается всегда, даже

если вы не ответили), у системы «едет крыша» и после первого же звонка она снимает вызов. Все. Вы блокиро-вали входящие звонки на вторую трубку.

- вы находитесь на одной соте, звонки идут сколько угодно на обе трубки, вы ответить не можете, второй говорит нормально. Вы регистрируете время прихода всех его звонков и как быст-ро он берет трубку (по факту прекра-щения вызова).

А теперь долгожданные коды:

- **Test Mode: 904059 [MENU]** Для того, чтобы выйти из этого режима, просто отключите батарейку.
- **Reset Counters: 904060 [MENU]** якобы сбрасывает все счетчики, не обнуляе-мые в обычном режиме. Можете ис-пытать на свой страх и риск.
- **Short Programming Mode: 987 [MENU].** На дисплее ваш 10-значный городской номер. Введите другой, просто нажмите [RCL]. На дисплее номер вашей системы. При необходи-

мости введите другой. Для окончания программирования нажмите [YES] или [SEND], для продолжения программирования оставшихся трех наборов [RCL].

- **Long Programming Mode: 923885 [MENU]** Методика та же, что и в коротком методе, только отображается еще куча всякой всячины, типа Initial Paging Channel, но нам это ничего не даст.

Процесс интуитивно понятен, хоть и различается в деталях для разных моделей, поэтому подробно его описывать не имеет смысла. Пробуйте сами. На всякий случай записывайте все значения перед тем, как их изменить.

#### Как расшить Motorola GP-68

Чуть ниже процессора, примерно около сантиметра, есть низкоомная перемычка (похожа на сопротивление). Ее надо удалить и станция сможет «покидать» режим памяти и предоставлять вам набор любой частоты прямо с клавиатуры от 136 до 174 МГц. Эта перемычка может быть замкнута каким-нибудь «дядькой» до вас, жирной каплей олова.

Для этого вам понадобятся очень чувствительные реле с током срабатывания около 10 мА и падением напряжения на обмотке, но не более 5 вольт.

Можно сделать и другую схему, работающую по тому же принципу, но в качестве развязывающих элементов применить оптроны.

При опущенных обеих трубках, постоянный ток АТС через обмотки реле не течет, так как внутри телефонного аппарата стоит развязывающая емкость (через нее к линии подключен звонок).

При поднятии трубки, на телефоне возникает ток, срабатывает реле и отключает аппарат. При этом, если на свободный вывод реле, отключающий один из аппаратов подать напряжение около 60 вольт (как напряжение ожидания со станции), то этот телефон становится приоритетным: если он отключен от линии, то подключен к эквиваленту линии и при поднятии на нем трубки все равно отключится второй телефон.

Обмотки реле шунтируются большими емкостями для того:

- чтобы реле не представляли сопротивления для частот голосового диа-

пазона;

- чтобы реле не срабатывали и не представляли сопротивления для вызывного сигнала (постоянная составляющая при этом гасится на внутренней емкости телефона 1 мкф);
- чтобы при наборе на одном аппарате не звякал звонок на другом.

Эксперименты показали, что достаточно электролитов 200 мкф. Но лучше побольше.

#### **Эмулятор SIM-карточки сотовых телефонов**

Как сделать маленький и автономный эмулятор SIM-карточки? Есть несколько путей.

1. Самый крутой путь — достать где-то чистые SIM карточки, которые предназначены для сотовых операторов. Правда, они не совсем чистые, на них должен быть уже зашит криптографический алгоритм COMP128, и надо иметь для этих карточек вразумительную инструкцию по программированию шифровального ключа Ki. Дело в том, что в разных SIM-карточках ключ может находиться в совершенно разных местах. Что касается криптографического алгоритма, то он тоже может прошиваться в

разных местах на карточке (нет единого стандарта, да он и ни к чему). Крипто-алгоритм (в данном случае COMP128) обычно находится в масочном ПЗУ карточки, и любой доступ к нему извне закрыт. Было бы, конечно, хорошо, если бы его можно было оттуда выдрать, но это невозможно!

Программа алгоритма написана на спец-ассемблере с применением других специальных средств и поэтому имеет чрезвычайно маленький объем (чуть более 1 Кб), для работы ей достаточно всего 128 байт ОЗУ.

Скорость вычисления результата 0.6 секунды (650 000 операций).

Программу ASIM мы не рассматриваем, так как для эмуляции SIM карточки она удобна только в «лабораторных» (домашних) условиях, но никак не в мобильном варианте!

2. В случае, если найдутся крутые программисты, которые смогут на ассемблере и с учетом специфических особенностей операционной системы процессорных смарткарт стандарта ISO 7816, реализовать опубликованный теперь, и ставший широким достоянием хакеров всего мира, алго-

ритм COMP128, так, чтобы после компиляции программа занимала не более 2 Кб и могла спокойно работать с оперативной памятью 128 байт, то останется только заняться поисками подходящего типа процессорной смарткарты (а в них обычно используется процессор 8051 или 6805 производства фирмы Motorola или SGS Thomson). При желании, можно доставать такие карты (чистые, без крипто-алгоритма DES или какого-либо другого) по средней цене 10-15 долларов за штуку. Эти карточки будут иметь процессор 6805 или 8051, ОЗУ 128 байт, ПЗУ 6 Кб, ППЗУ 3 Кб. В крайнем случае, можно достать более дорогие карты на базе процессора Motorola MC68HC05SC48 с ОЗУ 240 байт, ПЗУ 13 Кб и ППЗУ 8 Кб. Далее будем думать, как зашить в них эту программу крипто-алгоритма, шифровальный ключ Ki, а также мобильный номер IMSI.

3. Самый реальный путь — сделать эмулятор SIM карточки на куске текстолита, но без каких либо проводов, идущих на компьютер. На этой плате устанавливается несколько микросхем: процессор Atmel AT89C51 (или AT89C52), внешнее ОЗУ на базе флэш-памяти, внешнее ППЗУ 64 Кб. Туда зашивается уже широко известная и готовая немецкая программа

SIM\_EMU.EXE (43 Кб). Может быть ее придется немного доработать. Питание на эту плату эмулятора подается, естественно, от телефона.

## Двойники

В России двойников имеют следующие сотовые и транковые системы:

- AMPS/DAMPS (без защиты A-Key) — «Фора» (Петербург).
- NMT-450 (без SIS-кода) — Еще жив в Минске.
- MPT-1327 (транк) — АМТ, АСВТ.
- SmartTrunk (транк).

Не имеют двойников компании БиЛайн (протокол DAMPS IS-54) и МСС (протокол NMT 450i), так как применяются системы аутентификации: A-Key и SIS-code соответственно. В системе компании БиЛайн двойники возможны только на незащищенных роуминговых номерах.

Для создания двойника можно приспособить любой телефон, который может работать в системе, где работает телефон владельца. Для этого потребуется всего

лишь разобраться в управляющей программе хост-процессора телефона.

Для защиты от двойников в сети DAMPS может применяться протокол аутентификации A-Key, в сети NMT — система SIS (Subscriber Identity Security).

## **AKEY**

AKEY это тривиальное название системы аутентификации, используемой в сетях AMPS/DAMPS. Собственно AKEY представляет из себя восьмибайтовое число-ключ, хранящееся в сотовом телефоне абонента и являющееся уникальным для каждого абонента. AKEY вводится при продаже телефона клиента и хранится в базе.

AKEY не меняется и остается постоянным при нормальной работе телефона.

На основе AKEY (постоянный ключ) с помощью хеш-функции CAVE, используемой в качестве входных параметров, помимо AKEY, ESN, MIN телефона, а также случайное число, присланное по эфиру с базовой станции, генерируется временный ключ, называемый SSD\_A (тоже 8 байт). Этот ключ в дальнейшем и используется при аутентификации для генерации ответ-

ного значения. Постоянный AKEY не используется при аутентификации и служит только для расчета временного ключа.

При установлении соединения, система передает сотовому телефону случайное число, которое шифруется по алгоритму CAVE (Cellular Authentication and Voice Encryption) с использованием временного ключа SSD\_A и других уникальных параметров телефона (ESN, MIN) в качестве ключа. Ответ посылается на базовую станцию, которая, в свою очередь, независимо от телефона генерирует ответное число (все параметры телефона, в том числе и AKEY, и текущий SSD\_A, хранятся в базе на станции), и сравнивает его с полученным. В случае несовпадения числа, принятого от телефона с независимо посчитанным числом, аутентификация считается неудачной и телефону отказывается в соединении.

Периодически (примерно раз в неделю) станция посылает сотовому телефону сообщения о генерации нового временного ключа, SSD\_A, по получении этого сообщения (SSD\_UPDATE) телефон рассчитывает новый временный ключ SSD\_A, используя уже известный постоянный AKEY, ESN, MIN, и случайное число со станции. В ито-

ге, сам ключ аутентификации (SSD\_A) является временным и периодически меняется, и становится бессмысленным «клонирование» трубок (а также нахождение SSD\_A методом последовательного перебора), поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом.

### Как расшифровать АКод

Расшифровать АКод по посылкам со станции и ответам трубки можно только методом прямого перебора кодов, да и то с ограничениями. Функция **SAVE** является односторонний хеш-функцией с маленькой разрядностью выходного кода, поэтому вычислить ключ по данным, передаваемым по эфиру практически невозможно.

### Список процессоров, использующихся в трех популярных сотовых телефонах

#### Motorola

68HC11, DSP: AT&T16XX, MC566XX

#### Ericsson

ARM7TDMI core, DSP: Texas Instruments

#### Nokia

H8/XXX, Z80

### SIS

**SIS** (Subscriber Identity Security) — система аутентификации и защиты информации пользователей сотовой сети NMT-450i. Принцип действия SIS аналогичен AKEY: при запросе на соединение, станция посылает сотовому телефону случайное число, которое обрабатывается хеш-функцией SIS в телефоне с использованием 120-битового уникального ключа пользователя, часть результата хеш-функции посылается на базовую станцию для сравнения, другая часть используется для шифрования набираемого номера.

В отличие от AKEY, SIS не меняется и всегда остается постоянным для конкретного телефона, а также обеспечивает шифрование набираемого номера (в системе AKEY тоже предусмотрена возможность шифрования номера, однако она не используется в Российских системах). Также, в отличие от AKEY, SIS-код зашивается в телефон производителем и не может быть изменен провайдером услуг (AKEY обычно может вводиться с клавиатуры).

## Недокументированные возможности

Некоторые возможности современных сотовых телефонов были и остаются неизвестными для широкой публики. Оно пожалуй и правильно. Не всегда нужно, а порой и опасно это для стандартного потребителя. Но ряд наиболее простых и интересных функций, по моему, заслуживает того, чтобы ими можно было поделиться.

### Nokia 6110, Nokia 5110

- \*#0000# (Software Version, Software Date, NSE-3 = for use in GSM 900)
- \*#92702689# (Warranty Menu)
- \*4720# (activate Half Rate — less quality, but more battery capacity)
- #4720# (deactivate Half Rate)
- \*3370# (activate Enhanced Full Rate — better speech quality, less battery capacity)
- \*3370# (deactivate Enhanced Full Rate)

### Nokia 2110 (i), 2110e, 9000 (i), 8110, PT-11 и разновидности

Попробуйте набрать кнопками —

\*#170602112302# — на экране должна появиться версия софта, установленного в аппарате. В случае, если у вас версия позже 5.31, то наберите — \*#682371158412125#.

Кроме того, набрав \*#3283# или \*#DATE#, получите дату производства своей машинки. Для Nokia 1995 года это будет месяц и год, для 1996 — календарная неделя и год. С моделей начала 1996 года изменена раскладка клавиш — \*DATE# — \*#2172#. Для старых Nokia, можно попробовать \*#9999#. В модели — 8110 для выяснения версии софта просто наберите — \*#8110#. Для 3110, соответственно — \*#3110#. Для 3810 — \*#3810#.

Заодно уж, в связи с тем, что Security Code Generator для Nokia, давно перестал являться привилегией серьезных «фрикеров», а поступил и в распоряжение «чайников», было бы нелишним сменить код вашего аппарата. Речь идет о режиме «телефон», активирующем возможность использования чужой SIM-карты. В случае, если вы оставили предустановленный производителем код, он может быть легко взломан ибо имеет жесткую привязку к IMEI самого аппарата.

### Hagenuk Global

Для отображения версии ПО — ###\*21#. Как вариант — ##9140\*83#75\*2#.

### Motorola 8200 и разновидности

Нажмите и удерживайте кнопку \* до тех пор пока на дисплее не появится []. В итоге введите сочетание [[][]113[]1[] и просто нажмите ОК, этим вы включите Monitor-Modus. Сочетание [[][]003[]1[] и нажатие ОК удалит телефонную книгу из меню. Сочетанием [[][]003[]0[] вы вернете ее обратно. Таким же образом, но с цифрами 004 вы можете удалить пункт меню — **Сообщения**. С помощью [[][]008[]1[] и ОК можно добавить в меню установок пункт выбора линии при разговоре с двумя абонентами. Благодаря [[][]070[]0[] вы можете вернуть все установки вашего телефона в исходное состояние.

### Philips PR 747

Для вызова версии ПО попробуйте \*#8377#. Как вариант — \*#5644#

### Siemens S 4, Sony CM-DX 1000 и разновидности

Выбрав в меню опцию «информация» и нажав кнопку «выбор», вы получаете

идентификационный номер аппарата. Сразу после этого попробуйте набрать — 6573555, 6664867, 7684666, 7775978 или 8795777. Теоретически в результате вы должны получить дополнительную опцию в меню сеть, которая позволит вам обзавестись информацией о поле приема, используемом канале GSM и многое другое.

Для старых аппаратов попробуйте — 5553756.

### Siemens S1, S3, P1, Marathon и им подобные

Нажав сочетание Меню, 97 или 98, левую кнопку меню, 5553756, красную кнопку, вы должны получить доступ в служебную зону вашего аппарата. Для P1 — просто нажмите и удерживайте 8 до тех пор, пока не появится V, после этого просто нажмите #, появившиеся цифры, это версия ПО. Или для активации служебной зоны попробуйте нажать 5, удерживать до появления M, потом #.

### Siemens S6 и S10

К сожалению «Monitor-Modus» реализуется в этих моделях только с помощью дополнительного программного обеспечения.



Небольшим утешением может послужить хохма в S4 и S10, — внесите в телефонную книгу номер: +12022243121. И наслаждайтесь.

### **Ericsson GH 197/198, GH 337, 318/388, и им подобные**

Благодаря сочетанию — стрелка вверх, \*, стрелка вниз, стрелка вниз, \*, стрелка вниз, \*, вы получите доступ в служебную зону аппарата. Для GH337 — кнопку стрелка вверх, заменяет левая кнопка со стрелкой. Вниз — соответственно, правая. Или — стрелка вверх, \*, стрелка вниз, стрелка вниз, \*, стрелка вверх, \*.

В служебной зоне, вы можете получить информацию о состоянии вашего аппарата. Например, цифры 951024 1054, означают, что дата выпуска вашего программного обеспечения — 24.10.95, 10 часов 45 минут. Нажав любую кнопку, выбирайте дальнейшие опции. В режиме «Flash», можно стартовать аппарат по новой, если рухнет весь софт. Режим «Init EEPROM MMI» позволит вернуть все установочные значения в «начальное» состояние. «TEXT CHECK» — позволит отобразить на дисплее все 254 варианта сообщений на выбранном вами языке. И т.п.

### **Для всех (практически) аппаратов**

Для проверки «левоты» машинки попробуйте — \*#06# — будет вызван IMEI (International Mobile Equipment Identifier) и вы получите родной номер своего аппарата.

## **Прослушивание**

В настоящее время никакие системы сотовой связи не защищены от прослушивания. Аналоговые системы (NMT, AMPS, DAMPS в аналоговом режиме) без труда прослушиваются обычным приемником-сканером, который имеет возможность настройки на диапазон сотовой системы. Цифровые системы (DAMPS/TDMA, GSM) прослушиваются специально модифицированными телефонными аппаратами той же системы.

## **Дело было еще в конце 1993 года...**

### **Скука**

Дело было в конце 1993 года, бизнес с девчонками к тому моменту уже кончился. Жизнь и бизнес вернулись в обычное, скучное русло — выдушивание из иност-

ранцев денег на «русское программирование». Писать об этом отдельно не имеет смысла, потому что все было предельно цинично и скучно — якобы десяток русских программистов и художников были заняты в крупном программном проекте. На деле же все делал один студент, а разница между его зарплатой и получаемыми деньгами и была источником моего существования.

Все изменилось, когда выяснилось, что знакомый видеопират пользуется взломанным сотовым телефоном.

Взломанный телефон — это как? А так — звонишь ты, а платит кто-то другой (или вообще никто). Ты на время присваиваешь номер чужого телефона, и счет за твои переговоры приходит хозяину номера (в принципе, он может и отказаться платить за чужие разговоры).

### **Мой сегмент рынка**

Тусовка этого видеофила боялась бандитов как черт ладана, поэтому продвигала пиратчинку среди своих друзей, коммерсантов средней руки. У меня же, напротив, имелся вполне положительный опыт взаимодействия с этими самыми ужасными бандитами. Мне сразу стало понятно, что это

— идеальный товар для людей, занятых разнообразной незаконной деятельностью. Судите сами — никаких следов (звонишь с разных номеров), не подслушать (кого подслушивать-то?), да и объем звонков у таких людей, как правило, столь велик, что никаких денег на честный телефон не хватит.

Первое, что нужно было решить для себя, это где переделывать телефоны. Можно было воспользоваться услугами уже существовавшей тусовки, но такое решение привело бы к зависимости от них и их ценовой политики. Памятуя о том, что сделанное одним может повторить другой, я обратился к знакомому нищему электронщику.

### **Гений без штанов**

Знакомство с ним произошло за полгода до описываемых событий, когда изучался вопрос о создании перехватчика для автомобильной сигнализации. Потом расскажу об этом поподробнее. Пока что замечу, что она была создана, но наладить массовый сбыт — ввиду сложности использования — не удалось. Примерно во время нашего знакомства он продал свой телевизор и музыкальный центр, чтобы на что-то жить. Он сразу согласился стать главным

техническим специалистом. Еще бы — эта тема пахла деньгами.

Не то чтобы он действительно был гением. Со временем я понял, что 90% его крутости и «профессионализма» — просто понты. Но, надо отдать ему должное, он и его команда (всего 4 человека) обладали фантастической работоспособностью и решали-таки любые технологические задачи.

### **Реклама**

Для начала были извещены все специфические знакомые. Они узнали, что телефоны — отключенные за неуплату или со сложной судьбой — теперь можно не выбрасывать или отдавать детишкам. Теперь у них может появиться новая жизнь. Как обычно, этот контингент реагировал с гипертрофированным энтузиазмом. Именно в те времена появилась фразочка о «мешках телефонов». Реальность, как всегда, оказалась много скромнее.

### **Первый заказ**

Первый заказ пришел из тюрьмы. Ну, не совсем тюрьмы — из изолятора временного содержания. И волновали людей не деньги, а секретность. Помню, мы даже внутренности телефона протерли — уничто-

жали отпечатки пальцев. Не все шло гладко, но результат был! Клиент (а это была девушка, хозяйка агентства недвижимости) осталась очень довольна и рассказала своим знакомым. Заказы посыпались.

### **Первая фаза**

Сначала мы «делали» аппараты единственной на тот момент сотовой компании. Делали просто — подменяли номер внутри аппарата, прописывая другой, и все. Почти никакой защиты там не было. Номер хранился в энергонезависимой памяти (EEPROM) телефона. Раз разобравшись, как ее редактировать, мы уже легко повторяли операцию. Поначалу мы не продумали как следует ценовую политику и делали аппараты практически за бесценок — клиент платил один раз \$150 (кажется) и потом, за каждую смену номера, еще \$45.

Учитывая, что минута разговора по городу стоила \$3, цены были более чем божескими. Скоро стало ясно, что долго так продолжаться не может — мы неграмотно действовали, «выдавая» один и тот же номер сразу нескольким клиентам. В результате они мешали друг другу: система обладала смешным свойством — с данного номера звонить может только один человек.

Второй «срубает» первого с линии (я упрощаю, но эффект именно такой). Тогда мы и придумали вторую фазу.

### **Технология**

Пора объяснить поподробнее, как же это — пиратировать чужой номер. В случае, если неинтересно, можно смело читать следующий пункт. Ничего сверхзанимательного здесь нет, просто хочется все расставить на свои места. Пока мы обсуждаем систему NMT-450. В Москве аппаратурой этой системы пользуется Московская Сотовая (МСС), по России — это СОТЕЛ. В те времена телефонные аппараты системы NMT-450 были практически не защищены от взлома. Каждый аппарат в системе идентифицировался десятизначным кодом.

Расскажу о нем подробнее. Сразу хочу предупредить, что все это уже давно неактуально, потому что усилиями хакеров фирму Nokia вынудили разработать достойную систему защиты (SIS). Рассмотрим на примере Москвы. Допустим, у абонента номер телефона 8-гудок-2-900-4455 (совершенно случайно выбранный номер, не звоните туда!). Тогда в его аппарате могло быть прописано следующее: 480-4455-123, где 48 — код города Москва в системе NMT-450,

04455 — идентификатор собственно абонента (последние 5 цифр номера), а последние три цифры — защита.

Слабая такая защита. Дело в том, что обойти ее было проще простого — прописать туда три нуля (для продвинутых — «двоичных» нуля; если среди этих цифирей встречался ноль, он был «десятичным», то есть цифрой «А»). В итоге, чтобы «подсесть» на телефон знакомого с номером 8-гудок-2-905-1112, нужно было записать в свой аппарат 485-1112 (защиту мы даже не учитывали — всегда обнуляли).

### **Вторая фаза**

Целей у второй фазы операции было две: во-первых, облегчить жизнь клиентам, чтобы им не приходилось приезжать к нам за новыми номерами, во-вторых, нормализовать ценовую политику, то есть брать с клиентов больше денег.

Мы сделали так, что клиент теперь смог сам менять номер в своем телефонном аппарате. Стало очень удобно — кончились деньги у одного, «пересел» на любого другого. В некоторых моделях аппаратов оказалось достаточно немного подправить программу (это же компьютер, как ни крути),

для других было разработано специальное устройство, которое вставлялось внутрь и, как паук, подключалось к десятку контактов.

Цены мы тоже подняли — стали брать за модификацию аппарата от \$300 до \$400. Тут нужно заметить, что это мы брали столько, наши дилеры отрывались по полной программе — доходило аж до восьми сотен.

### **Кошмар**

Через каких-то 10 месяцев именно этим словом определялось состояние функционеров операторов NMT-450. В некоторых городах пиратов было почти 10%, а объем неоплаченных разговоров — все 90%. Это уже не говоря о недовольстве клиентов. В общем, стало пахнуть керосином. Операторам в крупных городах пришлось срочно менять оборудование и аппараты абонентам, чтобы перейти на систему защиты SIS.

### **Приколы**

Мы тяжело работали, но и веселья было предостаточно. С тех времен в обиходе остались несколько фраз. «Таскать телефоны мешками» — одна из них. Еще был прикольный случай, когда мы с приятелем

зашли на Модную Большую Биржу. Там торговали металлом, валютой и еще хрен знает чем. Зашли мы к знакомому Большому Функционеру. Оба — с пиратскими телефонами. Когда ему понадобилось куда-то позвонить, мы оба предложили наши трубки. Он замешкался (напоминаю, тариф был около \$3 минута), а мы ему и говорим: «Думаешь, мы платим?» Он, вероятно, решил, что мы — крутые бандиты и за нас платят какие-то люди. «Но ведь кто-то же платит!» — только и смог выдавить из себя Большой Функционер. Это фраза тоже осталась с нами навсегда.

### **Так кто же все-таки платил?**

Сложный вопрос. Сначала, пока операторы не поверили в саму возможность взлома, они не принимали претензий. Но со временем, когда жалобы стали массовыми, в офисе стали происходить эксцессы с рукоприкладством (ясно, кто мог себе позволить платить по \$3 в минуту?). Тогда операторы стали давать клиенту распечатку его звонков и просить его вычеркнуть незнакомые номера. После этого счет корректировался. Так все и устаканилось до момента, когда все 100% абонентов были переведены на защиту.

### **Что же они не пытались бороться?**

Все просто — никакого закона мы не нарушали, а наша крыша сразу договорилась с крышей сотового оператора (по их понятиям, «нельзя запретить вору воровать» или что-то в этом духе). В общем, чувствовали мы себя как сыр в масле. Наши клиенты тоже почти ничего не нарушали. Я сразу им объяснял, что, во-первых, доказать ничего нельзя, а во-вторых, даже если сознаться, то привлекут по двум нестрашным статьям административного кодекса — незаконное использование услуг и неразрешенный радиопередатчик. В общем, штраф в несколько МРОТов и все.

### **Ну защитились они, и что дальше?**

А дальше мы переключились на другую систему (AMPS/NAMPS/DAMPS), которая была защищена не намного лучше.

С введением защиты тема не умерла. Разумеется, мы знали о такой возможности и заранее к этому готовились. И вот, как сейчас помню, 1 апреля, в день, когда крупнейшие NMT-операторы заявили о 100% переводе своих клиентов на систему SIS, мы

сделали первый, пока пробный, выход в эфир пиратированного телефона другой системы. В этот раз повезло операторам, которые использовали телефоны стандарта AMPS, и его модификациям (NAMPS, DAMPS). В Москве это BeeLine (Билайн).

Тут особого ума не надо — их же хакают по всей планете! А вот и нет! То есть хакают, конечно. И 90% всех телефонов на земле именно этой системы. Но, во-первых, технология у американских фрикеров, мягко говоря, inferнальная. А во-вторых, несмотря на сотни криков, по делу в Internet так ничего и не нашлось. Только пустые разговоры и — редко-редко — взломанная управляющая программа из телефона какой-нибудь античной модели.

Дело в том, что американцы, когда создавали стандарт AMPS, думали головой, а не жопой, как европейцы со своим NMT. И защиту, какую-никакую, но заложили. Нужно заметить, что до нас по-хорошему, чисто, эту защиту никто так и не взломал. Все известные мне американские хакеры-фрикеры пользовались обходными путями.

И что же там была за защита? Для своего времени — очень даже неплохая. У каждого телефонного аппарата есть неизме-

няемый заводской серийный номер ESN (Electronic Serial Number). Он выдается раз и навсегда (технология не предусматривает его замену). При продаже телефона оператор заполняет NAM (Number Address Module), где хранится номер телефона и еще кое-какая техническая информация. Так вот, комбинация ESN и NAM и есть уникальный идентификатор абонента.

Для того, чтобы имитировать такой телефон (то есть подсесть на него), нужно знать ESN и NAM. Откуда можно взять эту информацию? Есть два способа — социально-инженерный и технологический. Первый — это trashing и подобные фокусы.

Trashing — это копание в мусоре, который выкидывают из магазинов, в надежде найти выброшенную копию контракта или что-нибудь еще (к примеру, номер чужой кредитной карты). К слову, в штатах мусор является федеральной собственностью, так что за копание в помойке можно схлопотать срок. В совке все проще.

Без мусора тоже можно обойтись — к примеру, снять девочку, которая контракты выписывает, и за шоколадки/секс получать от нее чужие секреты. Опытный жулик может таким образом обеспечить свои потреб-

ности, но коммерчески это неприменимо. Значит, остается второй способ — нужно искать технологическое решение. Тут тоже есть варианты. Можно купить промышленное устройство. Для этого нужно подделать бумаги, дающие право приобретать такое оборудование (абы кому такое не продают — только правоохранителям), и наскрести немалые деньги — товар штучный, цены — соответственно — атомные. И нужно понимать, что оборудование, которое можно купить таким образом, придумано и сделано для другого — это тестовое оборудование, которое заодно может и то, что требуется для взлома. Это примерно как вместо отмычки покупать гранатомет — препятствие в виде замка и двери будет устранено в обоих случаях. Так что лучше сделать такой агрегат самостоятельно.

### **Как?**

Тут-то и началось самое интересное. Выяснилось, что никакой полезной информации нет. В Internet'e удалось найти только самое общее описание, и оно содержало огромное количество неточностей и ошибок. Пришла пора рассказать обо всем подробно.

## **Технология, часть 2**

Опять же, если неинтересно, эту главу можно пропустить. Для интересующихся расскажу, как же оно действует. Разумеется, упрощенно, только то, что относится непосредственно к взлому. Взлом состоит из двух частей — сначала нужно чужую информацию добыть, и потом нужно ее записать в свой аппарат. Для установления связи аппарат сообщает о себе пару ESN+NAM (американские фриеры их так и называют — pairs). Базовая станция (в народе — сота) эту информацию принимает и запрашивает у главного компьютера, существует такая пара или нет. В случае, если существует, то соединение происходит. Здесь важно то, что пара передается в эфире как есть, то есть без кодирования. И ее можно перехватить. Для этого нужно сделать приемник и декодер. Вместо приемника можно использовать радио-сканер, только придется попотеть, чтобы найти нужный (в большинстве сканеров нужный диапазон закрыт). Дальше нужно декодировать принятый сигнал. Метод кодировки там — NRZ (non-return to zero). В аппарате нужно модифицировать программу так, чтобы он позволял несложно и оперативно менять ESN+NAM.

## **Ловилка**

Сначала мы сделали приемник. Мы не хотели связываться с поиском правильного радио-сканера, поэтому собрали приемник сами. Конечно, катушки никто не наматывал, все было собрано из модулей. Потом к нему подцепили персональный компьютер, и первый NRZ-декодер был просто программой под Windows (или DOS, не помню уже). Именно так мы получили первые пары. Попробовали. Получилось. Тогда сделали первую автономную ловилку — коробочку размером с пару видеокассет, с антенной, жидкокристаллическим окошечком на 4 строчки, и разъемом для подключения к последовательному порту компьютера (RS-232). Она перехватывала сигнал от любого телефона системы AMPS в радиусе 100-120 метров, показывала в окошке пойманный номер, ESN и еще кое-что, к взлому непосредственно не относившееся. С этой коробочкой мы объездили не один город. Она до сих пор где-то валяется как память, хотя почти сразу были сделаны более совершенные устройства.

## **Аппараты**

Потом руки дошли и до взлома аппаратов. Сначала возникла проблема с иден-



тификацией процессора, который жил внутри телефонов Motorola. Из общих соображений было ясно, что это, скорее всего, процессор той же фирмы. Однако модель удалось определить не сразу. Кажется, его звали MC68HC11A (впрочем, после стольких лет могу и ошибаться). Первое, что мы попытались сделать, это определить его цоколевку (то есть взаимное расположение ног). Это оказалось непросто — хотя в те времена Motorola уже начала выкладывать документацию на web, по закону подлости, именно этого процессора там не было. Тогда я вспомнил, что один мой приятель в Израиле работает на фирме Motorola. Я ему позвонил, он сходил в библиотеку фирмы, и через пару часов из нашего факса вылез требуемый документ. Работа закипела. Я написал простенький табличный дизассемблер и сделал табличку для нашего процессора. Электронщики возились очень долго, зато и результат превзошел ожидания — в аппарат можно было записать сразу 10 разных пар и быстро переключаться между ними.

### **Сбыт**

Работу с клиентами я с самого начала поставил на «ура». Результатом стало то, что

почти все наши старые клиенты пришли снова. При этом они и платили снова, никаких скидок (кроме символических) им не делали. Просто они прекрасно помнили, как это сладко — болтать часами на халяву. Вместе с нашим телефонным аппаратом клиент получал список пар (для простоты — список), строчек около 100. Когда текущий список заканчивался, всем раздавался новый. Списки составлял я. Люди, имевшие «честные» аппараты и боявшиеся получить чужие счета, стали спрашивать через друзей — можно ли исключить их номер из списка. «За деньги мы можем все» — говаривал, бывало, мой приятель — адвокат из Израиля. Так же отвечал и я. За какие-то \$100 номер телефона счастливчика навечно пропал из наших списков.

Телефоны продавались по \$600-\$800 за штуку. Спрос был так высок, что я с трудом успевал покупать сырье — отключенные за неуплату или проблемные трубки и микросхемы памяти (ROM, по-русски ПЗУ), куда прописывалась новая программа. Из-за того, что сырья катастрофически не хватало, пришлось покупать его за границей, и я освоил кардинг.

Дело дошло до того, что на офисе, где я сидел, появилась табличка — «Прием денег круглосуточно». Это было веселое время.

### **Дилеры**

С первым своим дилером я познакомился, прочитав его объявление в Релкоме (была такая сеть, еще до появления в России полноценного Internet). Он продавал телефоны. Я предложил ему переделывать телефоны у нас, он согласился, и работа закипела. Но это был единственный случай, когда кого-то нашли по объявлению. В остальных случаях мне помогали мои клиенты и крыша — все ездили на родину с телефонами, и всегда находился молодой деятельный парнишка, который разворачивал у себя в городе каналы сбыта. Наши телефоны долетали аж до Иркутска и Владивостока.

### **Реклама, часть 2**

Заодно с перехватом телефонных пар электронщики разобрались и с кодированием пейджером, а мы продавали результаты перехвата. Нужно отметить, что это было еще до выхода известного указа о спецтехнике. Именно это я и решил прореклами-

ровать. Заказов было не очень много, но контингент обращавшихся был что надо — мелкие торговцы, жулики, разнообразные службы безопасности банков. Большинству из них я впарил и по пиратскому телефону — согладалаи, как правило, сами отменные параноики. И идея звонить, не оставляя следов в своем счете, им нравилась.

### **Заграница**

Мы славно развернулись в России и ближнем зарубежье. Но не давала покоя мысль о том, что крупнейший в мире рынок — обе Америки — нами не охвачен. Но торговать там так же, как в России, не представлялось возможным. Здесь мы имели дилеров с ловилками в большинстве городов, которые осуществляли послепродажный сервис — давали номера. В Америке же борьбой с сотовыми пиратами занимается Секретная Служба тамошнего министерства финансов, поэтому встречаться с клиентом второй раз очень опасно. Не то чтобы они уж очень эффективно борются, но щетки надувают и пропаганду разводят нешуточную.

Когда стало ясно, что так торговать не получится, мы вернулись к идее, которую обсуждали с самого начала, но за ненадоб-

ностью не реализовали — засунуть ловилку в аппарат.

### Такого еще никто не сделал!

Электронщики засели за свои осциллографы и прочую дребедень, и через некоторое время вынесли вердикт — радиотракт внутри аппарата подходит для перехвата. На человеческом русском это значило — сканер на фиг не нужен, в качестве сканера будет выступать сам аппарат. Остался NRZ-декодер. Его ничего не стоило сделать программным, то есть внести еще изменений в код программы телефона. Но такое решение было бы слишком легко скопировать (а к тому моменту наши программы воровали все подряд). И мы выбрали аппаратное решение — на базе процессора Z8. Это теперь я рассказываю, что там стоял за процессор, тогда же мы его так корезжили напильником, что понять это было невозможно. Такую штуку хрен скопируешь. И, что интересно, ее так никто и не скопировал. Наиболее талантливая тусовка конкурентов просто создала собственное устройство с точно таким же интерфейсом. У них это отняло 1,5 года — было за что биться.

### Что же получилось?

Получилось в кайф! В кармане лежал телефон, и если в радиусе 30–40 метров (не 100–120, как в случае со сканером, но и этого более чем достаточно) кто-то звонил или кому-то звонили, он перехватывал пару, запоминал ее и говорил «пииииип». На экране появлялась надпись:

SCAN nn

где nn — номер ячейки. Это просто для понта сделали, чтобы веселее было. В аппарате было 100 ячеек памяти. В них накапливались пойманные пары. Самые свежие затирали самые старые. Каждый раз аппарат звонил с другого номера. Это обеспечивало абсолютную безопасность — кто заметит, что в его счете ОДИН непонятный звонок? Да никто! А если и заметит, то не будет кричать — подумаешь, ошибся. Еще наш аппарат отвечал на звонок почти вдвое быстрее стандартного. То есть, если взять себе какой-нибудь из пойманных номеров и раздать его друзьям, дозваниваться будут на наш телефон, а не хозяину. Сильно?

### И как там Америка?

Увы. С Америкой так и не заладилось. В Израиль аппараты уходили неплохо (их

там штук 40, наверное), а вот в Америке народ оказался слишком запуган — несколько штук из Чикаго вернули с криками «не работает», но быстро выяснилось, что они просто испугались. В Нью-Йорке живут несколько наших творений, но там и контингент соответствующий — push'еры (это которые наркотой торгуют) и угонщики автомобилей. Для них это не самое страшное преступление в жизни. Собственно, я и придумал, как выйти на пушеров — заставил своих знакомых в NY спросить у друзей, которые нюхают: «Где берешь, предложи туда это!» Так и было продано несколько штук. Дальнейший сбыт там был осложнен тем, что в крупных городах (Нью-Йорк, Чикаго, Лос-Анджелес) введена дополнительная защита, на перехват которой наш аппарат не был рассчитан. Зато он умел брать телефоны из городов, где есть защита — ему можно было сказать: коды городов 212, 515 — игнорируй.

### **Так что, зря вставляли ловилку?**

Нет, конечно! С появлением автономного аппарата сбыт увеличился в разы — многие скептически настроенные люди немедленно купили себе и друзьям. Раньше

они не хотели быть привязанными к спискам. Еще купило много народу из тех, кто много ездит по России и в Америку. В общем, все шло даже слишком хорошо. Операторы стандарта AMPS/NAMPS/DAMPS стонали.

### **Защита**

И они начали защищаться. Организационно с нами сделать было ничего нельзя. Поэтому борьба шла техническая. И конечно, самые сильные войны шли в Москве, где был крупнейший рынок. Сначала они ввели коды доступа к междугороду. Это была идиотская идея — мы эти коды перехватывали и публиковали в списках. Потом они перевели всех на систему DAMPS. Это те же яйца, но вид сбоку. Единственная проблема была с аппаратами — кроме нас переделать их никто не справился. В итоге, мы объективно выигрывали от введения защиты. И только через несколько лет Билайн разорился-таки на достойную защиту. Это так называемый A-Key (authentication key). В детали вдаваться не буду, скажу только, что и она не идеальна. Но именно с введением A-Key они смогли наконец вздохнуть свободно. В Москве пиратства больше практически нет. В других городах все по-

прежнему процветает. Только в Питере попытались что-то сделать, но денег на A-Key у них не хватило, и они купили защиту на базе так называемого RF fingerprinting («отпечатки пальцев» телефона). Система построена на базе одного мифа и мешает пиратам только в хорошую погоду. Чуть на небетучки — пиратские телефоны снова оживают. А из других мест вообще ничего не слышно о защитах.

## **Фрод**

Фрод — несанкционированный доступ к услугам связи, а также получение услуг в режиме неправомерного доступа.

По данным Международной ассоциации сотовой телефонии (CTIA — Cellular Telecommunications Industry Association), ежегодные потери от «двойников» у операторов стандарта D-AMPS/AMPS во всем мире составляют около 1 млрд. USD. Точные убытки российских операторов неизвестны. Типовые потери западного оператора от 3 до 5%. В июне 2000 года Ассоциация по борьбе с мошенничеством в области связи оценивала ежегодные убытки операторов и абонентов более чем в 12 млрд. USD.

Более 1,5 млн. обладателей мобильных телефонов ежегодно отказываются оплачивать выставленные счета. К такому выводу пришла консалтинговая компания Mummert+Partner. По ее данным, только в текущем году немецким компаниям мобильной связи придется списать на безнадежные долги около DM750 млн., что составляет примерно 3,5% от их годового оборота.

## **Основные виды Фрода**

**Access Fraud** — мошеннический доступ — несанкционированное использование услуг сотовой связи за счет умышленного или неумышленного вмешательства, манипулирования или перепрограммирования номеров сотовых аппаратов ESN (Electronic Serial Number) и/или MIN (Mobile Identification Number). В AMPS эти номера могут быть перехвачены при помощи сканера и использованы для программирования других телефонов — метод создания нелегального «двойника». Способ возможен на сетях без аутентификации. Защита основана на проверке записей звонков на предмет обнаружения почти одновременных звонков из разных зон; проверка с использованием «черных списков», а

также анализ статистики на «подозрительные события», прежде всего рост трафика абонента.

**Stolen Phone Froud** — мошенничество с украденным телефоном — несанкционированное использование украденного или потерянного сотового телефона. Способ работает как правило, пока владелец не известит компанию и та не заблокирует доступ с украденного телефона. Защита — блокировка клавиатуры паролем, немедленное заявление в компанию-оператор об утрате телефона, присмотр за телефоном.

**Subscription Fraud** — мошенничество с контрактом — указание неверных данных при заключении контракта, использование услуг в кредит с намерением не оплачивать их.

Способ работает при плохом качестве работы с клиентами, а также до момента, когда компания принимает решение о блокировке телефона. Защита — строгий кредитный контроль, введение предоплаты, «горячий биллинг» или «онлайн биллинг»; создание базы данных клиентов и контроль заявленной информации; создание «черных списков» недобросовестных клиентов.

## Некоторые системы для защиты от Фрода

**PhonePrint** (Corsair Communications Inc.) — комплекс распознавания радиотелефонов по радиоотпечаткам — Radio Frequency Fingerprint (уникальным характеристикам излучения передатчика каждого аппарата). Представители Fora Communications (AMPS), где PhonePrint был установлен в июле 97 года, утверждают, что система компании Corsair в целом работала успешно (стоимость составила около 1MUSD), однако уже в 98 году систему решили демонтировать и возратить компании-производителю. Около 1/3 клиентов, отказавшихся от услуг Fora, испытывали неудобства от «двойников» с клонированными аппаратами. Fora вместо этого установила систему A-Key. По-видимому, следует ожидать вспышек «фрода» на региональных системах, куда «перетекут» клоны из С.-Петербурга. Система PhonePrint была введена в действие в Казахстане на системе Алтел. В 1999 Corsair подписал соглашение с Comcel (Colambia) на поставку системы PhonePrint 5.0, которая позволяет одной системой антифрода обслужить сразу несколько систем сотовой связи. Состоялось подписание договора с ALLTEL — амери-

канским мультиоператором, обслуживающим более 6.5 млн. абонентов в 22 штатах. В случае, если абонент данной сети переходит в режим роуминга, к примеру, отправившись в другой город (при условии, что там также имеется система PhonePrint 5.0), то местная система отправит «радиоотпечатки» излучения телефона в его «домашнюю систему». Связь состоится только в случае, если и роуминговая система и «домашняя система» будут располагать однотипной информацией. В случае, если отпечатки совпадут, то звонок можно будет сделать. Несмотря на сложность сети, ожидание соединения для клиента не увеличивается, в то время, как любителей позвонить за чужой счет ждут трудные времена.

**Система A-Key.** Принцип работы: при включении радиотелефона компьютер сети передает на него случайное число. В телефоне число преобразуется по определенному алгоритму (CAVE — Cellular and Voice Encryption — американская технология шифрования аналогичная тем, что используется в военных целях) и направляется компьютеру (в HLR или AC — authentication Center). Компьютер выполняет те же действия с посланным числом, причем использует в качестве ключа то число, которое зара-

нее в него занесено, как соответствующее данному телефонному аппарату. Результаты — вычисленный и присланный аппаратом сравниваются. В случае, если результат совпадает, то телефон допускается в сеть. В каждом аппарате должен быть «зашифрован» индивидуальный A-Key. Поскольку A-ключ не передается в эфир, его нельзя перехватить и использовать, как это делалось с серийными номерами. Все новые телефоны уже снабжены A-Key, остальным клиентам нужно было обратиться в офис компании за бесплатным перепрограммированием. Около 4000 телефонов ранних выпусков не поддерживают систему A-Key, их требуется заменить на новые, от клиентов потребуются доплата.

AKEY — это тривиальное название системы аутентификации, используемой в сетях AMPS/DAMPS. Собственно AKEY представляет из себя восьмибайтовое число-ключ, хранящееся в сотовом телефоне абонента и являющееся уникальным для каждого абонента. AKEY вводится при продаже телефона клиента и хранится в базе. AKEY не меняется и остается постоянным при нормальной работе телефона. На основе AKEY (постоянный ключ) с помощью хеш-функции CAVE, использующей в каче-

стве входных параметров, помимо AKEY, ESN, MIN телефона, а также случайное число, присланное по эфиру с базовой станции, генерируется временный ключ, называемый SSD\_A (тоже 8 байт). Этот ключ в дальнейшем и используется при аутентификации для генерации ответного значения.

Постоянный AKEY не используется при аутентификации и служит только для расчета временного ключа. При установлении соединения система передает сотовому телефону случайное число, которое шифруется по алгоритму CAVE (Cellular Authentication and Voice Encryption) с использованием временного ключа SSD\_A и других уникальных параметров телефона (ESN, MIN) в качестве ключа. Ответ посылается на базовую станцию, которая, в свою очередь, независимо от телефона генерирует ответное число (все параметры телефона, в том числе и AKEY, и текущий SSD\_A, хранятся в базе на станции), и сравнивает его с полученным. В случае несовпадения числа, принятого от телефона с независимо посчитанным числом, аутентификация считается неудачной и телефону отказывается в соединении. Периодически (примерно раз в неделю) станция посылает сотовому теле-

фону сообщения о генерации нового временного ключа, SSD\_A, по получении этого сообщения (SSD\_UPDATE) телефон рассчитывает новый временный ключ SSD\_A, используя уже известный постоянный AKEY, ESN, MIN, и случайное число со станции. В итоге, сам ключ аутентификации (SSD\_A) является временным и периодически меняется, и становится бессмысленным «клонирование» трубок (а также нахождение SSD\_A методом последовательного перебора), поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом.

**Система SIS.** SIS — Subscriber Identification Security. Внедрение началось на сетях NMT450 с системы «Дельта Телеком» еще в 1994 году. С тех пор, как утверждает менеджмент компании, не зарегистрировано ни одного случая проникновения в сеть. Внедрение функции было сложным и дорогостоящим и включало: модернизацию аппаратного и ПО коммутатора; приобретение и внедрение аппаратно-программного комплекса; замену всех мобильных аппаратов, не имевших встроенной функции SIS; модификацию ПО базовых станций. Соответствующая реализация стандарта известна под названием NMT450i. Помимо функции



защиты от фрода, оператор получает ряд дополнительных возможностей, к примеру, пониженный тариф для телефона с ограниченной (одной сотой) мобильностью, ограничение зоны обслуживания для конкретного абонента, SMS и ряд других. Основное преимущество — возможность организации автоматического роуминга.

Принцип действия SIS аналогичен AKEY: при запросе на соединение станция посылает сотовому телефону случайное число, которое обрабатывается хеш-функцией SIS в телефоне с использованием 120-битового уникального ключа пользователя, часть результата хеш-функции посылается на базовую станцию для сравнения, другая часть используется для шифрования набираемого номера. В отличие от AKEY, SIS не меняется и всегда остается постоянным для конкретного телефона, а также обеспечивает шифрование набираемого номера (в системе AKEY тоже предусмотрена возможность шифрования номера, однако она не используется в Российских системах). Также, в отличие от AKEY, SIS-код зашифруется в телефон производителем и не может быть изменен провайдером услуг (AKEY обычно может вводиться с клавиатуры).

**Система FraudBuster.** Система обнаружения фрода и формирования профиля абонента предназначена для обнаружения и борьбы в том числе и с новыми видами фрода. Система способна накапливать данные о вызовах каждого конкретного абонента и создавать на этой основе индивидуальные профили каждого абонента. Они затем дополняются, анализируются по мере совершения новых звонков и способны немедленно обнаруживать аномальную активность, которая может свидетельствовать о факте фрода. Поскольку инфраструктура не связана с концепцией системы защиты, то она подходит для систем GSM, AMPS, CDMA, TDMA, iDEN.

**Система Signature Fraud Management System** (Signature FMS) от Lucent Technologies — новое ПО, которое может использоваться операторами, как проводной, так и беспроводной связи. Система способна динамически в реальном времени оценивать отклонения в поведении абонентов с целью обнаружения действий, характерных для злоумышленников.

## Трюки с пейджером

Все приколы с пейджерами можно разделить на две категории: приколы над владельцем пейджера и приколы над операторами, которые принимают твои сообщения.

Как отправлять сообщения? Во-первых, ты можешь просто позвонить оператору и надиктовать ему сообщение — этот способ отправки нужно использовать при приколах над операторами (когда диктуешь очень сложные слова или несешь полный бред). А второй способ передачи сообщений — это отправка их через Internet с какого-нибудь пейджергейта. О них подробнее.

Пейджергейты — это такие сервера, заполнив форму на которых, ты можешь отправить сообщение на любой пейджер без участия оператора. Это удобно, когда ты сидишь в Internet, и единственная телефонная линия занята, или если ты хочешь отправить очень много сообщений за раз без напруга (типа, пейджер спам). Лично я пользуюсь (и тебе советую) двумя серверами: <http://send.ru> и <http://www.pagergate.ru>. На этих серваках представлены практически все операторы России (и не только). Теперь о том, как ими пользоваться.

В случае, если посмотреть глазками — все сервера по отправке сообщений похожи друг на друга. Сначала выбираешь нужную страну и город. После твоего выбора, скорее всего, произойдет перезагрузка страницы и появится список доступных операторов для конкретного города. Теперь тебе нужно выбрать оператора. В случае, если ты не знаешь его название, но знаешь первые три цифры телефона, ты можешь легко найти по ним нужного тебе оператора. Тут наступает самая ответственная часть: введи номер нужного тебе абонента и свое сообщение. В случае, если ты отправляешь сообщение через сенд.ру, то у тебя появится возможность указать дату отправки сообщения. То есть отправить сообщение не сейчас же, а спустя некоторое количество времени. Написал? Отправляй!

Ну а с отправкой сообщений через оператора не должно возникать никаких проблем.

Таким образом, братишка, приступим. Ты звонишь оператору (или заходишь на сайт), называешь номер своего друга/подруги/... и начинаешь диктовать сообщение. Специально для тебя я отобрал самые прикольные сообщения, которые сильно разве-

селят обладателя пейджера и повесят на-  
мертво (так что тремя пальцами не ожи-  
вишь) бедного оператора. Вот они:

Что ты смотришь на меня – это я,  
твой пейджер.

Коля, мне домой не звони. Я у тебя.

Паша, если хочешь, я дома. Вова.

У меня Наташа. Не могу прокормить.

Привет. По-моему, у нас с тобой бу-  
дет маленький. Твой пейджер.

Или сперва отправляешь такое сооб-  
щение:

Идет подготовка к отключению вашего  
пейджера.

А через минуту:

Теперь питание можно отключить!

А эти сообщения надо отправлять по  
очереди с небольшим интервалом.

Переключи пейджер в режим вибрации.

Положи пейджер в передний карман шта-  
нов.

Ты чувствуешь, как сильно я тебя люб-  
лю?

Димулька. Я жду тебя дома и пригото-  
вила тебе вкуснейший супчик! Вася.

Саша, не спеши – бабушку уже стошни-  
ло!

Мой ноги, я уже в дороге. Маша.

Митя, подъедешь ко входу, зайди ко  
мне сзади.

Марина, мы у тебя дома. В случае, ес-  
ли вздумаешь приди, пожалуйста, пре-  
дупреди нас!

Поимей для разнообразия совесть, по-  
звони мне. Катя.

Милый, ты знаешь, в чем фишка? Твои  
носки лежали на столе у меня дома.

Буду поздно. Суп на полу – вытри.

Я жду тебя в ванной. Срочно.

Дима, чем удобряли, то и выросло!

Купи, пожалуйста, туалетную бумагу и  
приезжай домой срочно!

Ты забыл у меня свой пейджер, приез-  
жай – заberi.

В случае, если ты научишься выгова-  
ривать следующее предложение и продик-  
туешь его оператору, то это будет просто су-  
пер:

Леша, скажи маме, какие лекарства на-  
до купить: анизоилированный активатор  
комплекса стрептокиназы и плазминоге-  
на, а еще нужна билатеральная саль-  
пингоофорэктомия.

Также ты можешь использовать такие  
словосочетания:

● острая воспалительная демиелинизирую-

щая полирадикулонейропатия

- диссеминированная гонококковая инфекция
- этилендиаминтетраацетат
- эндоскопическая ретроградная
- холангиопанкреатография
- идиопатический гипертрофический субортальный стеноз

## GSM-безопасность

Немецкая компания Rohde & Schwarz, занимающаяся с мая 2001 года криптографией для Siemens, создала самую «продвинутую» криптографическую систему для GSM-телефонов.

TopSec GSM («самый безопасный GSM» — скромно, но со вкусом позволит бизнесменам, политикам, военным и вообще любому желающему общаться по самым безопасным каналам.

Для демонстрации системы использовался популярный сотовый телефон Siemens S35i, немного усовершенствованный микросхемой, выполняющей кодирование данных. После усовершенствования

телефон «научился» использовать комбинацию «1024-битного асимметричного и 128-битного симметричного кодирования», что, по словам представителей Rohde & Schwarz, является самой безопасной системой шифрования.

После набора номера пользователю остается лишь нажать специальную кнопку, включающую собственно использование этой криптографической системы. Кроме того, связь при этом возможна только с другим аналогичным устройством, оснащенным модулем TopSec GSM или поддерживающем эту функцию.

Правда, некоторые аналитики уже высказали недоверие к этой системе. Основой для сомнений является наличие собственной криптографической системы в GSM-сетях, которая, вроде бы, предоставляет достаточный уровень защиты (в конце концов, совсем уж секретные вопросы лучше решать при личной встрече. Кроме того, сотовые операторы обязаны предоставлять правоохранительным службам возможность прослушивать звонки, к примеру, подозреваемых. То есть, у оператора в любом случае должны быть возможность прослушать разговор, независимо от уровня шифрова-

ния. В любом случае, TopSec GSM вряд ли в ближайшее время станет общераспространенной системой. Дело в том, что используемые в системе схемы шифрования превышают допустимые значения для ряда стран. То есть импорт подобных телефонов в некоторые страны будет запрещен, либо для их использования понадобится специальное разрешение (почти как со сверхмощными компьютерами).

## Приложения

### Толковый словарь

**AMPS**

Advanced Mobile Phone System — усовершенствованная мобильная телефонная служба, аналоговый стандарт сотовой связи.

**AMSS**

Aeronautical Mobile Satellite Service — спутниковая система мобильной авионавигации

**Bluetooth**

Технология, позволяющая осуществлять беспроводную передачу сигналов на короткие дистанции между телефонами, компьютерами и другими устройствами.

**bps**

bits per second — скорость передачи данных, количество информации в секунду.

**BSIC**

Base Station Identity Code — код идентификации базовой станции

**Call barring**

Запрет вызова

**Call divert**

Переадресация вызова (то же самое, что и call forwarding)

**Call forwarding**

Переадресация вызова (то же самое, что и call divert)

**Call hold**

Удержание (сохранение) вызова

**Call waiting**

Ожидание вызова

**CDMA**

Code Division Multiple Access — множественный доступ с кодовым разделением.

**Cell**

Сота, ячейка

**Cell site**

Совокупность базовых станций, установленных в одном месте

**Cellular**

Сотовый

**Clearinghouse**

Расчетный центр

**Closed user group**

Закрытая группа пользователей

**Conference call**

Конференц-связь (то же самое, что и multiparty call).

**D-AMPS**

Digital AMPS — цифровой AMPS. В настоящий момент известен как TDMA.

**DCS**

Digital cellular system — цифровая система сотовой связи.

**DECT**

Digital Enhanced Cordless Telecommunications — цифровой стандарт беспроводной телефонии, установленный ETSI.

**dual band**

Двухдиапазонный мобильный телефон, способный работать на разных частотах.

ных диапазонах, к примеру, GSM 900 и GSM 1800.

**dual mode**

Двухстандартный мобильный телефон, способный работать в разных сетях, к примеру, в CDMA и AMPS, GSM и DECT.

**EDGE**

Enhanced Data rates for GSM Evolution — технология, разработанная для стандартов GSM и TDMA, которая позволяет удовлетворять требованиям 3G — передачи большого количества информации на большой скорости (384 кбит/сек).

**EFR**

Enhanced Full Rate — улучшенное качество речи. Поддержка данной функции должна осуществляться как телефоном, так и оператором связи. Допускает передачу данных до 14400 кБит/с.

**ЕРОС**

Операционная система мобильных терминалов, разработанная Symbian.

**ERMES**

European Radio Messaging System — единая европейская пейджинговая сеть, работающая в Европе, на Среднем Востоке и в Азии.

**ESN**

Electronic Serial Number — электронный серийный номер.

**ETACS**

Extended Total Access Communication System — аналоговая мобильная сеть Великобритании, есть доступ также в Европе и в Азии.

**ETSI**

European Telecommunications Standards Institute — Европейский институт стандартов электросвязи.

**FCC**

Federal Communications Commission — Федеральная комиссия связи (США).

**FDMA**

Frequency Division Multiple Access — множественный доступ с разделением по частоте.

**FSS**

Fixed Satellite Service — стационарная (фиксированная) система спутниковой связи.

**GMPCS**

Global Mobile Personal Communications by Satellite — Глобальная спутниковая система персональной мобильной связи.

**GPS**

Global Positioning System — Глобальная система определения местоположения.

**GPRS**

General Packet Radio Service — технология беспроводной передачи пакетных данных на больших скоростях (115 Кбит/сек).

**GSM**

Global System for Mobile Communications — Глобальная система мобильной связи, цифровой стандарт мобильной связи.

**GSM 1800**

Цифровой стандарт GSM на частоте 1800 МГц, известен также как DCS 1800 или PCN, используется в Европе, в Тихоокеан-

ских странах Азии, Австралии, России.

**GSM 1900**

Цифровой стандарт GSM на частоте 1900 МГц, известен также как PCS, используется в США, Канаде, отдельных странах Латинской Америки и Африки.

**GSM 900**

Цифровой стандарт GSM на частоте 900 МГц, распространен в более 100 странах Европы и Азии.

**GSM MoU Association**

Международная Ассоциация операторов стандарта GSM.

**Handheld**

Ручной абонентский терминал

**Hand-off, hand-over**

Передача вызова от одной базовой станции к другой в процессе передвижения пользователя.

**HSCSD**

High Speed Circuit Switch Data — технология передачи данных на повышенных скоростях (до 57 Кбит/сек) в стандарте



**GSM.**

**IMEI**

International Mobile Equipment Identity — международный идентификатор аппаратуры мобильной связи.

**IMSI**

International Mobile Subscriber Identity — международный идентификатор абонента мобильной связи.

**IMT-2000**

International Mobile Telecommunications-2000 — международная система мобильной связи 2000, мобильная телефония третьего поколения.

**IN**

Intelligent Network — интеллектуальная сеть.

**IP**

Internet Protocol — протокол работы Internet.

**IPR**

Intellectual Property Rights — Права на интеллектуальную собственность.

**IS-41**

Внутрисетевой протокол соединения сетей США как цифрового так и аналогового стандарта.

**IS-54**

Первоначальный цифровой TDMA стандарт. введен в 1992 году, затем в 1996 году модернизирован до цифрового стандарта IS-136.

**IS-95/cdmaOne**

Цифровой стандарт мобильной связи, основанный на технологии CDMA.

**IS-136**

Цифровой стандарт мобильной связи, основанный на технологии TDMA.

**ISDN**

Integrated Services Digital Network — цифровая сеть с интеграцией функций, позволяет осуществлять высокоскоростные передачи голосовых данных, информации или видео посредством существующих линий инфраструктуры.

**ISO**

International Standards Organization — Международная организация стандартов.

**ITU**

International Telecommunications Union — Международный союз электросвязи.

**LMDS**

Local Multipoint Distribution System — в США стандарт для высокоскоростной передачи голосовых данных и информации, используется для установки беспроводной связи в пределах компании или здания.

**LPC**

Linear Predictive Coding — кодирование (речи) на основе метода линейного предсказания.

**LTP**

Long Term Prediction — долгосрочное предсказание.

**MAHO**

Mobile Assisted Handoff (Handover) — передача обслуживания с участием подвижной станции.

**Mobile (station)**

Подвижная станция (абонентский терминал).

**MPE-LTP**

Multi-Pulse Excited Long Term Predictor — линейное предсказание с многоимпульсным возбуждением и долгосрочным предсказателем.

**MSS**

Mobile Satellite Service — мобильная спутниковая связь.

**MTSO**

Mobile Telephone Switching Office — центр коммутации (обычно в применении к аналоговым системам сотовой связи)

**Multiparty call**

Конференц-связь (то же самое, что и conference call).

**NMT**

Nordic Mobile Telephony — мобильный телефон северных стран, стандарт сотовой связи, был введен в начале 1980-х годов в Швеции, Норвегии, Финляндии и Дании, впоследствии в некоторых странах Европы, на части территории России, на Среднем Востоке и Азии.

**OMC**

Operation and Maintenance Center — центр управления и эксплуатации.

**PBX**

Private Branch Exchange — офисный коммутатор (АТС).

**PCN**

Personal Communications Network — сеть персональной связи, известна также как DCS 1800 или GSM 1800.

**PCS**

Personal Communications Service — система персональной связи, обобщающее название для сотовых сетей США стандарта GSM 1900.

**PCSS**

Personal Communications Satellite Services — услуги (функции) спутниковой персональной связи.

**Penetration**

Проникновение — доля населения, пользующаяся сотовой связью (обычно выражается в процентах).

**PHS**

Personal Handyphone System — система персонального ручного телефона (японская система беспроводной связи).

**Pico Cell**

Малая сота в сети мобильной связи, устанавливаемая для увеличения емкости внутри зданий.

**PIN**

Personal Identification Number — персональный идентификатор (абонента сотовой связи).

**PMR**

Private Mobile Radio — радиосвязь ограниченной группы пользователей (к примеру, команда экстренной помощи).

**PSTN**

Public Switched Telephone Network — коммутируемая телефонная сеть общего пользования.

**PUK**

Personal Unblocking Key — персональный ключ разблокировки.

**РТТ**

Производное от Ministry of Post, Telecommunications and Telegraph, используется для обозначения ведущего оператора в стране.

**RCR**

Research & Development Center for Radio Systems — Центр исследования и развития радиосистем (Япония).

**Roaming**

Роуминг — процесс автоматической регистрации мобильного телефона в другой сети при перемещениях. Международный роуминг — возможность регистрации при нахождении за границей.

**Router**

Маршрутизатор — блок управления соединениями между различными сетями, идентифицирует адреса данных при прохождении, определяет путь передачи данных и формирует пакеты данных для дальнейшей передачи.

**Satellite phone**

Спутниковый телефон.

**SDH**

Synchronous Digital Hierarchy — стандарт цифровой передачи данных.

**SIM**

Subscriber Identity Module — модуль идентификации абонента GSM-сети (SIM-карта, или смарт-карта).

**SMS**

Short Message Service — функция (услуга) передачи коротких сообщений.

**SPACH**

SMS, Paging and Access Response Channel — канал передачи коротких сообщений, вызова и ответа на вызов.

**Switch**

Коммутатор (центр коммутации).

**Symbian**

Совместное предприятие Motorola, Nokia и Psion, разработчик операционной системы EPOC.

**TACS**

Total Access Communications System — общедоступная система связи (стандарт содовой связи на частоте 900 МГц, распространен в Великобритании).

**TCH**

Traffic Channel — канал трафика.

**TDD**

Time Division Duplex — дуплексное разделение во времени.

**TDMA**

Time Division Multiple Access — множественный доступ с разделением во времени, цифровая технология основана на стандарте IS-136, современное обозначение стандарта D-AMPS.

**TETRA**

Trans European Trunked Radio — общеевропейская система транковой связи (стандарт транковой связи).

**3GPP**

Third Generation Partnership Project — глобальный проект совместной координации разработки WCDMA институтами стандартизации стран Европы, Японии, Южной Кореи и США.

**TMSI**

Temporary Mobile Subscriber Identity — временный идентификатор абонента мобильной связи.

**Triple mode**

Трехстандартный мобильный телефон, который может работать одновременно в аналоговом режиме на частоте 800 МГц и в цифровом режиме на частотах 900 МГц и 1900 МГц.

**UMTS**

Universal Mobile Telecommunications System — универсальная система мобильной электросвязи, стандарт сотовой связи третьего поколения в Европе, разработанного ETSI.

**UWC**

Universal Wireless Consortium — объединение разработчиков и операторов стандарта сотовой связи IS-136.

**VAD**

Voice Activity Detector — детектор речевой активности.

**VLR**

Visitor Location Register — гостевой регистр (база данных, содержащая сведения об абонентах-роумерах).

**WAP**

Wireless Application Protocol — бесплатный не лицензированный протокол

беспроводный связи, позволяющий создавать расширенные системы мобильной телефонии и получать доступ к страницам Internet с мобильных телефонов.

**WARC**

World Administrative Radio Conference — Всемирная административная конференция по радиочастотам.

**WCDMA**

Wideband Code Division Multiple Access — цифровой широкодиапазонный стандарт, охватывающий Internet, мультимедиа, видео и прочие высокочастотные приложения.

**WIN**

Wireless Intellectual Network — беспроводная интеллектуальная сеть.

**WLL**

Wireless Local Loop — беспроводное подключение телефона дома или в офисе к фиксированной телефонной сети.

**WOS**

Wireless Office System — технология, позволяющая пользователю переводить звонки на мобильный телефон.

**Использованные материалы****Globalstar: спутниковая система персональной связи**

Михаил Евсиков, Сергей Матвеев.

**Беспроводные средства связи и безопасность**

Виктор Иксар

**Алгоритмы шифрования надежны только в теории**

Элен Месмер

**Тайны маленькой синей коробочки**

Рон Розенбаум

**Техно Авангард: старое железо на новый лад**

Александр Соркин. kibizoid.da.ru. kibizoid@mail.ru

**Стандарт исключений для роботов**

Standard for robot exclusion. Martijn Koster, перевод А. Аликберова. Martijn Koster, m.koster@webcrawler.com.

**Butthead Style — с факом по жизни**

KibiZoid (kibizoid@mail.ru). kibizoid.da.ru.

**Задняя сторона Аськи: узнай, кого ты склеил**

KibiZoid (kibizoid@mail.ru). kibizoid.da.ru.

**Complete Modem Reference**

Held, Gilbert — 1996

**High Speed Cable Modems**

Azzam, Albert — 1997

### **Голосовые возможности модемов**

<http://home.novoch.ru/~ovchin/>

### **Модем для плохих линий**

Журнал «3D NEWS». Автор: LIKE OFF

<http://nap.newmail.ru>

### **Голосовые возможности современных модемов**

Максим Потапов. <http://www.rusdoc.ru/index.shtml>

**«Руководство для хакера» или самые свежие мысли о том, как развлечься на выходные**  
W.S.U.

*Научно-популярное издание*

**Серия книг «Tips and Tricks»**

**Жуков Сергей Михайлович**  
**Хакинг мобильных телефонов**

Налоговая льгота

«Общероссийский классификатор

ОК 005-93-ТОМ2 953000 — Книги и брошюры»

Подписано в печать 31.05.2006. Формат 70х100/32. Бумага  
газетная. Кол-во п.л. 7. Тираж 3000 экз. Заказ № 328.