Серия книг «Мой мобильный телефон»

М.С. Букин

Всё про Ваш мобильный телефон

Книга 3

Москва

Майор
Издатель Осипенко А.И.
2004

УДК 621.396.65
ББК 32.884.1–5
Б906

Серия основана в 2004 г. Осипенко А.И.

Букин, Максим Сергеевич.
Б906 Всё про Ваш мобильный телефон. Книга 3 / М.С. Букин. – М. : Майор, 2004. – 208 с. – (Серия книг «Мой мобильный телефон»). – ISBN 5-98551-003-4.
Агентство CIP РГБ

В книге рассказывается о дополнительных мобильных сервисах — оказывается, с помощью сотового телефона можно не только говорить, но и играть в казино, узнавать свое будущее и даже знакомиться. Отдельный раздел посвящен секретным GSM-услугам и вопросам безопасности. После прочтения книги вы станете продвинутым пользователем, разбирающимся в реалиях сотового мира XXI века.

ISBN 5-98551-003-4

От автора

Телефон — не роскошь, а средство коммуникации. Руководствуясь этим простым принципом, люди бизнеса первыми оценили прелести настоящей мобильности и принялись таскать с собой повсюду неслабые такие связные чемоданчики ради одной светлой цели: всегда быть на связи. Сейчас связь уже не требует от людей былых жертв и энергетических затрат, но прогрессивные люди по-прежнему идут впереди планеты всей, уверенно сжимая в руках важный атрибут — мобильный телефон. В этой книге вы найдете полный спектр информации о современных телефонах, узнаете стратегию поведения операторов сотовой связи, проникнете в такие интересные места, как калл-центр, опытную зону 3G, узнаете побольше о sms, wap- и java-играх, sms-мире БиОнЛайн и сможете понять, как использовать мобильный банк. Технологии не стоят на месте — в этой книге мы рассказываем о самом интересном в мире мобильной связи.

Нетрадиционные мобильные технологии

Секретный GSM

Предоставление услуг сотовой связи для государственных структур и федеральных служб безопасности — выгодный и стабильный бизнес. Для операторов это показатель надежности и стабильности, для госструктур — реальная экономия, так как строить собственные базовые станции на территории всей страны и покупать множество технического оборудования экономически невыгодно. Однако самое главное — обеспечить безопасность и конфиденциальность переговоров. Несмотря на заявления о том, что GSM-стандарт — самый защищенный из всех созданных к настоящему времени, специалисты перестраховываются.

Есть два основных направления обеспечения передаваемой информации — контроль сети и специальные абонентс-

кие терминалы. Кроме стандартного GSM-шифрования спецслужбы применяют свои технологии. Во всем мире давно и успешно разрабатываются и внедряются защищенные абонентские терминалы. История разработки берет начало первых месяцах 2000 года, когда шведская телекоммуникационная компания Sectra получила от Министерства обороны Швеции заказ на поставку защищенных от прослушивания GSM-телефонов Tiger. Несколько тысяч подобных «игрушек» и сейчас стоят на вооружении шведской армии, норвежских вооруженных сил (специально адаптированные для НАТО), полиции, на таможне, в правительстве и т. д. Цена каждого образца около 2 тысяч долларов, что ненамного дороже персональных спутниковых терминалов: безопасность стоит таких денег. Мобильные GSM-телефоны Sectra Tiger гарантируют защищенную передачу голоса, данных и SMS — функционируют в любой доступной сети GSM, но независимо от сети или оператора, используют средства криптографии на всем пути от отправителя до получателя. Вместе с тем, телефон имеет встроенную функцию DECT, что позволяет подключиться к обычной телефонной розетке в случае уничтожения врагом GSM-передатчиков, как шутят в компании Sectra.

После этого, в 2001 году, был анонсирован TopSec GSM («самый безопасный GSM»), который позволял любому желающему общаться по самым безопасным каналам (стоимость — $2 700). 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. 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 поддерживающим эту функцию. Однако проблема в том, что используемые в системе схемы шифрования настолько хороши, что превышают допустимые значения для ряда стран. Т. е. импорт подобных телефонов в некоторые страны будет запрещен, либо для их использования понадобится специальное разрешение (почти как со сверхмощными компьютерами).

Летом 2002 года озаботилось собственной безопасностью Агентство Национальной Безопасности США и сертифицировало GSM-телефон для правительственного использования. Счастливчиком оказался аппарат «Sectera» подразделения компании General Dynamics (GD Decision Systems). По телефону можно обмениваться информацией с грифом «Совершенно секретно». Фактически это трехдиапазонный (900/1800/1900) телефон Motorola Timeport со специальным криптомодулем — «скрэмблером». В заявлении офиса NSA по безопасным технологиям для конечного пользователя (Office of Secure End-User Technologies) сертификация названа важным достижением в стратегии правительства по обеспечению безопасности устройств беспроводной связи. Телефон совместим с беспроводным терминалом Sectera от General Dynamics, анонсированным в апреле. Терминал представляет собой компактное устройство, присоединяемое к проводному телефону для обеспечения конфиденциального обмена данными. GD планирует представить коммерческую версию своего секретного GSM-телефона и, возможно, он появит-

ся и в России — компания намерена продавать телефон не только в США.

Но самый лучший образец производят отечественный умельцы. Для российских военных, спецназовцев, оперативных структур безопасности изготовлен специальный сотовый телефон стандарта GSM-900/1800. Сотовые трубки (речевой шифратор и органы управления), которые производит НТЦ «Атлас» (подведомственное предприятие ФАПСИ), представляют собой аппарат, похожий на обычный мобильный телефон, только больших размеров, с массивным корпусом. Кроме того, в комплект входит базовый блок (радиомодем стандарта GSM плюс аккумулятор), который можно установить в машине, либо поместить в сумку, носимую на плече. Устройство имеет несколько степеней защиты, в том числе криптографических — помимо стандартной SIM-карты сотового оператора, в телефон вставляется еще и специальная смарт-карта российской разработки. На ней записана вся информация об алгоритме шифрования, причем количество ключей шифрования составляет невообразимую величину — 10 в 77-й степени. Нажав на специальную кнопку, абонент переводит связь в зашифрованный режим. После разговора смарт-карту можно из телефона вынуть. Если враг захватит телефон, без смарт-карты он по нему позвонить не сможет.

В экстремальных условиях пользоваться сотовым телефоном удобно — гораздо удобнее, чем, например, рацией. Поэтому весьма привлекательно выглядит идея оснастить российских военных этим популярным средством связи (к примеру, в Чечне есть действующие базовые станции сети GSM). У спецтелефонов, разработанных в НТЦ «Атлас», есть много интересных функций. Например, обязательная аутентификация собеседника — имя, фамилия, отчество. Или блок

питания, который можно подзаряжать от аккумулятора БТР (в отсутствие бронетехники можно подзаряжаться и от обычного автомобиля).

Однако хорошие телефоны — только половина дела. Чтобы напрочь исключить возможность перехвата разговоров, спецслужбы в России планируют создать сеть конфиденциальной сотовой связи в стандарте GSM. Она должна устранить межведомственную разобщенность силовых структур — таких, как Минобороны, ФСБ и МВД, снабдив их абонентов единым средством защищенной радиосвязи. По планам в 2003–2005 гг. эта система будет развернута в Южном, Центральном и Северо-Западном федеральных округах, а в 2005–2007 гг. — охватит всю территорию России. Скорее всего летом этого года можно ожидать постановления правительства о развитии системы конфиденциальной сотовой связи. В частности, в нем будет прописана процедура выбора базового оператора для ее создания. Сейчас ФАПСИ совместно с ФСБ и Минсвязи готовят материалы для проведения закрытого конкурса по выбору базового оператора.

Надо отметить, что первый фрагмент федеральной подсистемы конфиденциальной сотовой связи в стандарте GSM с мая 2002 г. действует в Чечне. Проект реализовали «МегаФон» и ФГУП «Космическая связь», которое обеспечивает спутниковый канал для соединения чеченского фрагмента с основной сетью сотового оператора. До начала 2003 г. чеченская сеть «МегаФона» обслуживала лишь военных и спецслужбы, а с февраля начались подключения и коммерческих абонентов. Инициатором создания конфиденциальной GSM-сети по всей стране выступает ФАПСИ, на которое возложено обеспечение информационной безопасности в ней.

Красивый Pre-Paid

Карты предоплаты — лицо оператора сотовой связи. Они попадают в руки абонента гораздо чаще, нежели рекламные буклеты или листовки. Многие наверняка слышали, что существуют любители, которые собирают карты, используемые в телефонных атвтоматах. Теперь такие филокартисты могут пополнить свои коллекции и оригинальными картами предоплаты сотовых операторов.

Такие карты называются еще скретч-картами из-за того, что имеют на оборотной стороне уникальный многосимвольный пин-код, защищенный отрывной лентой или специальным восковым покрытием, которое можно удалить ребром монеты. Материал, который служит основой для изготовления подобных карт — пластик, реже — особый по химическому составу плотный картон. Все карты имеют логотип компании-оператора, номинал, индивидуальный номер, на тыльной стороне есть инструкция по активации и штрих-код. По большей части они одноразовые — стер защитный слой, активировал карту, и она бесполезна для дальнейшего использования.

История пластиковых карт для оплаты за сотовые переговоры берет начало со специальных таксофонных телефонных карт. Именно на картах Московской и Санкт-Петербургской телефонных сетей создавался рынок коллекционирования — каждая из компаний за год выпускает до 60 разных дизайнов карт, причем в последние годы коллекционирование таксофонных карт стало завоевывать себе популярность

и в России. Таксофонные карты компаний обладают прекрасным дизайном, что обеспечивает им популярность среди российских и зарубежных коллекционеров. Сотовые компании пока не торопятся выйти на этот рынок — дизайн их карт преследует обычные цели для массовой продукции — выделиться из рядов конкурентов по простому признаку отличия, отразить различные номиналы карты, указать, для чего и как предполагается использовать этот кусочек пластика. Возможно, для возникновения концептуальных тенденций по авторскому дизайну у крупных сотовых компаний должно пройти несколько лет. Пока художественная и эстетическая сторона изображений, размещаемых на центральной стороне карт, невелика. По идее, изображение должно привлекать внимание, быть объективно интересным и привлекательным. Но примеры, демонстрируемые компаниями МТС и Вымпелком, пока относятся скорее к технологичному, унифицированному дизайну — максимум технического оформления, нет различий в оформлении между картами, кроме номинала. Соответственно, карточные продукты не обладают персональной узнаваемостью (или она не очень велика), и множество наименований и номиналов смешиваются в безликую серую массу.

Как говорит европейский дизайнер полиграфической продукции **Энтони Джерс**, «дизайн карты влияет на отношение к продукту, — приятно или не очень держать карточку в руках, насколько интересно покупать карту именно такого номинала. Безусловно, жизнь пластика для пополнения баланса сотового телефона недолговечна (неважно, Россия это или Германия, Великобритания...) — она используется только один раз. Да и решение о приобретении карты принимается не по виду карты, а по надежности и удобству. Но не надо

много денег, чтобы сделать этот процесс приятным. Нужно всего лишь немного фантазии и чувства меры. Хотя для этого сотовые операторы должны, наверное, больше подумать о своих пользователях. Ведь не секрет, что восприятие дизайна карты — это дело вкуса. Чем приятней внешний вид, тем чаще будет хотеться проводить платежи».

Однако некоторые подвижки заметны уже сейчас — с появлением авторских карточек для оплаты сотовой связи московской сети «МегаФон» может зародиться и новое хобби — коллекционирование сотовых карточек. Пластиковые карты первой серии оформлены в стиле «банкнот», с гравюрными портретами великих людей в области телекоммуникаций — Сэмюэла Морзе, Александра Белла и Александра Попова. В дальнейшем «МегаФон» будет периодически менять дизайн карт всех номиналов, выпуская памятные серии на различные темы. Это решение уже привлекло внимание российских и западных коллекционеров. Новые карты сети «МегаФон» упакованы в прозрачную пленку, под которой находится также удобный вкладыш с полезной информацией для абонентов и занимательными историями по тематике серии (в первой серии — рассказы о великих изобретателях).

Как отмечают специалисты на Западе, дизайн карт рождается долго. Обычно телефонные карты можно разделить на три основных сегмента рынка: артистические, туристические и рекламные. Говорят, что туристические телефонные карты — это ноу-хау французов. Париж — Мекка туристического бизнеса. Каждый год туда приезжают миллионы туристов, половина которых поддается соблазну купить и увезти на родину миниатюрную телефонную карту с достопримечательностями Парижа, его окрестностей. Чаще всего туристы увозят с собой неиспользованные карты. Получается,

что французские телефонисты торгуют воздухом. Сотовые компании могут выпускать карты, посвященные не только историческим объектам, но и историческим событиям (юбилей города или государства, круглая дата какого-либо события), праздникам, крупным международным событиям (олимпиада, фестиваль, крупное концертное турне). Самое главное — не перенасыщать карту деталями, иначе люди не смогут сконцентрироваться на карте и она не найдет отклика в душе коллекционеров.

По мнению художника Виктора Арефьева, карты даже одной компании можно оформлять по-разному. «Необходимо придерживаться общего стиля, а деталями можно улавливать конкретную группу потребителей — 10- или 20-долларовые карты, как самые массовые номиналы, надо оформлять в более жизнерадостном стиле, их покупают все слои населения. Карты среднего номинала (около 50 долларов) надо делать строгими, консервативными, внушающими уважение. Дорогие карты (100 и более долларов) должны выглядеть дорого, надежно, так как это продукт не для массового использования. На всех картах обязательно должны присутствовать фотовые картины — это приятнее для восприятия, чем однотонный кусок пластика с логотипом оператора. Однако этот рисунок должен быть пропечатан четко, так как полиграфическая «размытость» очень раздражает».

Самым большим спросом на Западе пользуются тематические карты с историческими миниатюрами, художественными и культурными памятниками, постановочными фотографиями красивых девушек или детей, снимками природы, животных. Этим давно пользуются западные операторы сотовой связи — их карты, созданные известными компаниями Schlumberger, Gemplus, (Франция), Solaic, Orga (Германия) —

стимулируют хорошее настроение. Очень много позитивных пейзажей, архитектурных памятников, футуристических изображений знаменитых художников и стилизованных зарисовок из жизни. Возможно, по прошествии небольшого времени и российские операторы примут на вооружение положительный опыт западных коллег — благо в России есть очень хорошие дизайнеры и художники.

Мобильные казино

Как известно, азарт человека не зависит от темперамента, профессионализма и материального положения. Наклонность к игре на деньги заложена в нас еще с детства. И все-таки — зачем люди ходят в казино? Наверное, чтобы получить приятные ощущения, проиграть энную сумму кровных, словом, с пользой провести время. Не беда, что рулетка — это по сути простейший генератор случайных чисел от 0 до 36, «однорукий бандит» — та же рулетка, но в иных ипостасях, что джек-пот выпадает крайне редко и только по большим праздникам. Главное — удовольствие от брызг шампанского, от приятных улыбок красивых девушек. Красота зеленого стола, разноцветные фишки, прыжки шарика на поле рулетки — это то, ради чего люди посещают казино.

Несколько лет назад, с появлением более-менее защищенных каналов передачи информации, начали появляться онлайновые казино с игрой на настоящие деньги. Отличная графика, приятная анимация, реалистичные звуки, азарт и опасность проигрыша создают ощущение присутствия за реальным столом. Но времена меняются, и вот уже sms и wap-казино

завоевывают рынок азартных клиентов. Причем данные тенденции наблюдаются по всему миру.

К примеру, израильский провайдер Zone4Play еще полгода назад объявил о своем использовании системы игр казино, разработанной для провайдера мобильной связи Orange. Интерактивная система вместе с другим комплектом услуг предоставляет подписчикам широкий выбор возможностей: различные игры казино — такие, как слот-автоматы, видеопокер, блэкджек, рулетка и другие. Приобретая виртуальные фишки, пользователи смогут насладиться азартными играми в безопасной среде. Развитие этой игровой системы, на базе различных технологий мобильной связи (беспроводного интернет-доступа (WAP), системы коротких сообщений (SMS), интерактивной голосовой связи (IVR)) и передовых технологических разработок (микро-приложения JAVA (J2ME), а также многообразной графической микробазы для мобильных устройств (GVM), подтверждает стабильность и широту выбора средств пользовательского обеспечения. Программа задействует технологии обеспечения прямого мобильного или интернет-доступа клиента к различным системам. Благодаря системе записи истории игр возможен выбор соответствующего уровня, качества игры; доступны интерактивные призовые состязания.

Такие же услуги развивает британский оператор мобильной связи Virgin Mobile — там уверены, что будущее сотовой связи немногим отличается от настоящей сети Интернет, с огромным изобилием казино. Подумывает о введении похожих услуг и оператор мобильной связи Vodafone. А в Европе все большую популярность приобретает так называемый сервис M-gambling (мобильные азартные игры). В Амстердаме, к примеру, действует лотерея, в которую выигрывает каждый

2400-й участник. По стоимости чуть большей доллара со своего мобильника можно отправить sms-сообщение. В ответ приходит информация, которая содержит порядковое число. При удачном раскладе можно заполучить неплохой приз (например, современную модель Apple). Вполне вероятно, что вскоре через мобильные казино огромные состояния будут переходить из одних трепещущих от волнения рук в другие, дрогнувшие от неожиданной удачи.

В нашей стране возможности пока немножко скромнее. Чтобы клиенты имели возможность получать игровые ощущения в офисе, на пляже, на природе — словом, там, где есть покрытие сотовой сети, — некоторые независимые фирмы решили реализовать наиболее популярные азартные игры в sms- и wap-формате. Правда, до сих пор проблема защиты данных, передаваемых между телефоном и сервером игры, не решена полностью, поэтому игры ведутся либо на «фантики» — условные очки, количество которых лишь символизирует удачливость игрока, либо на реальные деньги, помещаемые клиентом на счет провайдера подобных услуг.

Одним из наиболее ярких примеров является проект SMSCasino — здесь можно играть в классические игры казино посредством мобильного телефона. Причем, это реальная игра на реальные деньги. Для того чтобы начать игру, достаточно иметь любой телефон стандарта GSM, подключенный к одному из трех национальных операторов мобильной связи — БиЛайн, МТС или МегаФон, причем по любому тарифному плану, в котором доступна услуга SMS. Игра происходит посредством отсылки и приема SMS-сообщений. Сейчас доступны такие игры, как Блэк Джек, Рулетка, Покер. Правила совпадают с классическими, принятыми в большинстве традиционных казино. При регистрации на каждого игрока

заводится личный игровой счет. Немаловажной особенностью Мобильного игорного дома SMSCasino является простота и удобство способов пополнения игровых счетов и получения выигрышей. Пополнение игровых счетов происходит посредством активации предоплаченных карт номиналом в 500 руб., 1000 руб. и 3000 руб.

Однако стоит помнить, что WAP-терминалы не предназначены для отображения большого количества графической информации, и анимация графики осуществляется с трудом. Памятуя об этом, многие виртуальные мобильные казино попытались сделать процесс игры более быстрым, без необходимости загрузки больших объемов графики на терминал. Результат для рулетки выглядит следующим образом: клиенту выдается приглашение ввести либо число, на которое он ставит (1:36), либо диапазон чисел 1..18 и 19:36 в случае ставки 1:2; либо диапазон чисел 1..12, 13..24, 25..36 в случае ставки 1:3. После выбора клиент «крутит рулетку», то есть подает серверу игры команду сгенерировать случайное число, и в зависимости от этого числа и выбора клиента сразу происходит распределение денег.

Любимый многими Black Jack выглядит несколько более привлекательно: для него не требуется создавать анимацию, а вполне достаточно перерисовывать сцену игры (попросту говоря, экран) раз в шаг. Схема игры такая: сначала возникает экран с двумя открытыми картами клиента и с закрытыми картами дилера. Если клиент хочет, он может подать запрос на новую карту, в противном случае, дилер раскрывает карты. Эта игра очень просто реализуется, и большинство разработчиков мобильных игр уже включили Black Jack в свою «обойму».

Однако количество мобильных казино сейчас переживает фазу роста из-за крайне медленного приучения клиента тратить деньги именно таким образом. Проигрыш клиента должен быть компенсирован острыми ощущениями, удовольствием от игры, азартом, чего не наблюдается ни у одной реализации мобильных азартных игр. Существующая инфраструктура онлайновых казино, несомненно, поглотит своего младшего собрата, но не для извлечения прибыли, а для комплекта, «чтобы было». Имеющиеся WAP-телефоны позволяют играть в игры «на бегу», а в азартные игры надо играть спокойно.

Мобильные устройства, обладающие большим цветным экраном, функцией MMS и, что очень важно, собственной памятью и пространством для запуска Java-приложений, несомненно, станут намного более предпочтительной платформой для подобного рода игр — они будут придавать игре остроту и азарт. Однако их тотальное распространение на рынке обязательно должно сопровождаться надежными механизмами защиты он-лайновых транзакций с использованием мобильных терминалов. Но до той поры разработчикам мобильных азартных игр не раз еще придется набивать шишки, а самим играм — завоевывать свое место на рынке.

Мобильные знакомства

Всегда хочется чего-то нового, прелестного и красивого. В компьютерный век люди не разучились мечтать, и все так же хотят романтических увлечений, которые пробуждают полет фантазии или творческий взрыв необычайной силы.

Только теперь для того, чтобы познакомиться с красивой девушкой, совсем не обязательно даже выходить на улицу — все стало значительно проще, и одновременно с этим сложнее. А для начала взаимоотношений достаточно мобильного телефона и небольшого количества денег на электронном счету.

Психологи заметили, что разговор по телефону примерно в три раза сложнее, чем общение лицом к лицу. Разговор по электронной почте — в восемь раз сложнее. Все связано с тем, что мы не видим лица собеседника, не можем понять его невербальных сигналов, которые составляют до 70% получаемой информации. Поэтому успешно знакомиться и продолжать отношения с помощью электронных коммуникаторов могут только очень продвинутые пользователи с хорошим чувством языка, большим чувством юмора, не пугающиеся при выражении своих положительных и негативных эмоций, умеющие быть вежливыми и тактичными, обладающие высоким интеллектом и хорошими коммуникативными способностями. В любом другом случае общение будет протекать короткими репликами типа «как дела» и немедленно затухнет после того, как темы о погоде и молодежной моде будут «перетерты».

Есть несколько основных правил, выполнение которых поможет найти внимательного и приятного собеседника. Во-первых, будьте внимательны — надо всегда помнить имя или ник своего партнера по общению и никогда их не путать. Во-вторых, смотрите, куда отправляете sms-сообщения — часто по самой банальной невнимательности они уходят совсем не тому адресату, которому бы хотелось. В-третьих, развивайтесь интеллектуально — всем приятно говорить с человеком, у которого большой словарный запас,

который обладает широкой эрудицией и специальными знаниями в любой области, у которого есть обоснованное мнение и который может составить целостное впечатление о событиях и явлениях. Главное, чтобы было интересно. В-четвертых, будьте инициативны и по-хорошему непредсказуемы — можно набивать по sms стихи Есенина, Баладжарова, Талькова, сонеты Шекспира или хокку, можно отправлять красивые анимационные картинки с цветами, можно делать смешные фотографии и пересылать их по MMS. Ломайте стандарты, пишите свои впечатления от увиденных событий, проявляйте фантазию, и люди к вам будут тянуться. В-пятых, улыбайтесь. В-шестых, искренне интересуйтесь собеседником — его внутренним миром, настроением, ощущениями, впечатлениями, целями. Чтобы узнать человека, надо спрашивать — учитесь задавать правильные вопросы и уметь видеть ответы. В-седьмых, будьте вежливы, всегда вежливы и старайтесь разнообразить разговор и уйти от стандартных, стереотипных фраз и клише типа «что делаешь», «как прошел день», «все ок». Это убивает всякую романтику и ведет отношения к завершению по причине тотальной скуки.

Сейчас в мобильных знакомствах нет ничего противоестественного — особенно в наше время, когда воздух больших городов пропитан нереальными соединениями, от которых моментально плюхнулась бы в обморок любая тургневская девушка, когда магазины полны «продуктов», никогда до этого не порождавшихся природой, когда люди ежедневно пьют горстями одни таблетки, чтобы нейтрализовать действие других. Наш мир — мир мегаполисов, предъявляющий совершенно запредельные требования к нервной системе и ко всему человеческому существу в целом. Темп современной

жизни порождает нагрузки, к которым миллионы лет естественной эволюции так и не смогли бедного Хомо Сапиенс подготовить. А сотовые телефоны есть почти у 23 миллионов россиян — среди них много интересных и хороших людей, которые с радостью расширят свой круг знакомств с помощью мобильных средств связи.

Давно ушел в прошлое стереотип о том, что на службы знакомств (через мобильные телефоны и Интернет) заходят только объевшиеся гамбургерами очкарики-программисты и пускают слюни на старых дев, выложивших на сайт свою «выпускную» фотку. По большей части с помощью мобильных телефонов пытаются познакомится действительно хорошие люди. В мобильном и интернет-пространстве есть большая открытость и доверчивость, невероятная в обычной компании. И часто в мобильном чате вы можете получить отклик, сочувствие и одобрение, которого, возможно, вы никогда не имеете в реальной жизни, среди хорошо знающих вас людей. А не получили вы его, например, в силу застенчивости, закрытости, сниженной комумникативной активности или комплексов, связанных с вашей личной историей. Мобильная сеть позволяет творить нам свои жизни — здесь вас совершенно справедливо пожалеют, похвалят и расскажут, какая у вас необычайная душа. С вами могут построить сказочный мир на основании или безотносительно к вашему имени.

Во многом мобильный чат или хорошая служба знакомств — это место реализации насущной и плохо удовлетворенной в нашем индивидуалистическом и эгоистичном мире потребности в одобрении, поддержке, тепле, уважении, нежности, внимании и даже любви. Причина необычной для реального мира открытости людей в чате происходит от безопасности, которую дает вымышленное имя, невидимая внешность и

никому не известная личная история — особенно ее неудачная часть. Конференция или мобильный чат быстро становится местом, как минимум, флирта и, как максимум, дружбы и даже любви. Ведь в мобильной сети ваш виртуальный партнер хочет представиться вам таким, чтобы понравиться, вызвать одобрение, интерес, симпатию, любовь. Сеть снимает коммуникативные барьеры, и люди раскрываются — именно там можно отметить дивную доброту или недюжинный ум, нежность, благородство, верное сердце и дивные мечты безотносительно к возрасту, месту проживания, достижениям и отношениям со старшими. Жизнь часто доказывает, что реальность оказывается намного сложнее, чем наши представления о ней, порожденные зачастую расхожими штампами. И случается, что непредвзятый взгляд на вещи может сотворить удивительное превращение.

История развития, или как это работает

Все начиналось с sms — у многих операторов сотовой связи даже сейчас остаются сервисы, где все взаимодействие идет только с помощью коротких текстовых сообщений. В самом простом виде создается база данных, куда пользователи заносят самые простые данные о себе — возраст, рост, вес, цвет глаз и волос, интересы. Остальные могут устроить поиск и отобрать себе людей по этим критериям, зачастую очень формальным и поверхностным. После выбора с каждым собеседником можно пообщатся опять же с помощью текстовых сообщений или, при желании, голосом. Фотографий и голоса увидеть заранее невозможно, так как большинство телефонов не смогут отобразить не то что цветную, но и даже самую простую черно-белую фотографию. Поэтому —

только строчки симолов. Подобные службы называются Мобильные знакомства, SMS-флирт, SMS-знакомства — и есть у любого оператора из «Большой тройки» GSM. Тарификация каждого sms-сообщения стоит от 1 до 5 центов, причем, чтобы поговорить с приглянувшимся собеседником, понадобится несколько десятков таких сообщений. Особой регистрации для этого сервиса не требуется (логин и пароль присылаются на sms), сервис находится у оператора в разделе Развлечения.

Расширение технология получила с использованием wap — тогда появилась возможность делать более интерактивные базы данных, пользователи смогли оперативно редактировать свои анкеты или общаться с помощью группового или индивидуального чата. Специальной стоимости за такую услугу в этом варианте нет, оплата идет только на трафик по тарифам, действующим у каждого конкретного оператора. Также операторы сотовой связи предусмотрели возможность полностью голосовой службы знакомств — можно зарегистрироваться в базе данных службы «Знакомства» через оператора. Для этого надо заполнить анкету и оставить номер мобильного телефона. Для поиска надо указать пол, возраст, внешние данные и увлечения предполагаемого собеседника, и по этим параметрам система подберет одну или несколько кандидатур для общения. Сведения из базы данных доступны всем зарегистрированным на сервисе абонентам, вне зависимости от способа подключения. Стоимость минуты в таком случае будет равна 1 доллару.

Есть и новые технологии, которые сделают процесс знакомства более приятным — MMS-знакомства. Сейчас только компания МегаФон в московском регионе предоставляет та-

кую услугу — это служба знакомств с расширенными возможностями: можно обмениваться SMS-сообщениями и даже фотографиями. Конечно, для каждого пользователя есть своя анкета, но ее можно редактировать не только с мобильного телефона, но и через Интернет, добавлять туда фотографии, которые сможет просмотреть любой владелец MMS-телефона. Это значительно упрощает процесс взаимной «притирки» и увеличивает шансы найти действительно то, что хочется. Ведь лучше один раз увидеть, чем слышать и читать много-много раз. Стоимость услуг определяется за каждое sms-сообщение — от 5 центов за отправку запроса на поиск анкет, до 39 центов за заказ дополнительной MMS-информации об авторе анкеты.

В самое ближайшее время нас ожидают знакомства на базе услуг глобального позиционирования — можно будет выбирать собеседника не только по многочисленным критериям, но и по тому, насколько далеко он находится от вас. Стандартную фразу «Девушка, можно с Вами познакомиться?» теперь заменяет sms, которая приходит только тем, кто этого действительно очень ждет. Может, это судьба?..

Мобильная астрология

Стремление понять неизведанное, узнать свое будущее или правильно загадать желание (так, чтобы оно точно сбылось) — было свойственно человеку издавна. Мобильные телефоны только сделали этот процесс более надежным — получить свой гороскоп можно вне зависимости от настроения астролога, а растолковать сон помогут специально

составленные программы — в любом случае достаточно просто отправить sms по нужному номеру телефона.

У абонентов сотовых сетей есть шанс узнавать свое будущее на регулярной основе. Нет, не специальный человек, а машина, компьютер теперь занимается рассказом о том, что произойдет в самое ближайшее время. И не стоит ждать от нее ласки, внимательных глаз и спокойного баритона голоса — она не смягчит новости, а вывалит все сразу и без обиняков: «Доктор сказал в морг — значит, в морг»). Отправьте sms на нужный номер и получите ответ — деньги со счета списаны, все претензии к абонентской службе. Сухо, быстро — как на конвейере. С другой стороны, это приятно — можно попросить слепок будущего из любой точки мира, и будет стоить это совсем недорого, читать приятно, и вообще это достижение современного прогресса — узнавать о том, что случится, с разных точек зрения: хотите — как говорит китайский гороскоп, хотите — как европейский (потом будете ломать голову и думать, что было более правильным). Да все еще от дня недели и знака Зодиака, оказывается, зависит!

Итак, если Вы абонент МТС, то для заказа отчета о своем будущем надо просто определить, как часто Вам хочется узнавать эти приятные (или негативные) новости — ежедневно или все-таки раз в неделю. В зависимоти от этого надо выбрать периодичность канала в системе MTS-Extra и регулярно пополнять свой баланс, так как удовольствие совсем не бесплатное. Если интересно знать, что будет каждый день — завтра, то можно выбрать всего из двух гороскопов — Общий и Любовный. Жаль, что нет прогноза по индексам курсов акций, а то 15 центов за каждое sms окупились бы моментально. С другой стороны, никакими деньгами не купить

хорошее настроение — так что те же 15 центов за понимание того, с какой стороны и с каким выражением лица стоит подходить к любимой женщине — это совсем даже и недорого. Если интересные новости есть желание узнавать только раз в неделю, то не обойтись без еженедельных прогнозов (там уже 2 sms-сообщения общей ценой в 30 центов) — зато есть больше возможности точно определить свою жизнь. Гороскопы предоставляются по темам «Общий», «Семья-любовь», «Бизнес», «Автомобильный» и «Здоровье». Особенно приятно знать прогноз автомобильной ситуации персонально для своего знака Зодиака — вот было бы здорово, чтобы такие прогнозы были на 100% точными, — тогда бы и страховка для железного коня была без надобности. Кстати, для особо забывчивых или просто фанатов астрологии есть возможность за 65 центов заказать себе логотип со своим знаком Зодиака и носить его постоянно на сотовом телефоне.

Если есть желание услышать живой голос астролога, лучше, конечно, позвонить по телефону 0839 и услышать авторские гороскопы от президента Русской астрологической школы Александра Зараева. Преимущества, по сравнению с услугой MTS-Extra, в том, что свежую информацию можно получить не только на день и на неделю, но и на год вперед. Правда, это удовольствие «влетит в копеечку» — аж 60 центов (без учета НДС) в минуту, а поговорить астрологи горазды.

Вымпелком предлагает целый ворох астрологических и околоастрологических сервисов. Здесь тезис «к гадалке не ходи» вполне актуален — окромя реальной, есть SMS-гадалка, причем, в отличие от бледных и староватых бабулек, эта система просто монстр, так как умеет работать не только с хрустальным шаром (это уже анахронизм в наш компьютерный век),

но и грамотно раскидывает картишки (gadalka taroinfo), всякие-разные древные руны (gadalka runainfo), и даже предсказывает будущее с помощью книги перемен путем гадания по гексаграммам (gadalka geksainfo). И все это одновременно и без ошибок — причем, для использования услуги не надо приходить в полночь на старое кладбище — достаточно просто послать на короткий номер 684 SMS следующего содержания — GADALKA. Услуга вступит в диалог с пользователем, предлагая ему определиться со способом гадания <A> — по картам Таро, <D> — по рунам, <W> — по Книге Перемен. <AD> — дополнительная информация. Для ответа на вопрос надо послать на номер 684 SMS, состоящее из соответствующей буквы в угловых скобках, но бекз скобок (к примеру, для гадания по Книге Перемен: W). Кстати, при выдаче результата гадания в начале результата всегда расположены буквы, при помощи которых можно вступить в диалог с другим любителем гаданий. Для этого их просто надо послать на 684:. К примеру, выпало: <PT> РУНА «ЧЕЛОВЕК». «Осознайте свое существование. Вы — часть мироздания. Развивайте свое «Я», но отвергайте эгоцентризм». Для начала диалога следует послать на 684: PT.

Если замучили страшные кошмары и нет никакой возможности самому интерпретировать события в тонкой, цветной пленке сна, лучше обратиться к соннику. Однако перечитывать старые книги с пожелтевшими листками и поминутно чихать от пыли, напрягать глаза от мелкого шрифта и непонятного оглавления — удовольствие не очень. Гораздо лучше обратиться к услуге Сонник, которая с помощью современного мобильного телефона проинтерпретирует все описания сна. Для начала диалога на тот же номер 684 надо отправить SMS с содержанием SONNIK. К примеру, описание

сна идет таким словом — «SONNIK волосы», тогда сонник вступит с Вами в диалог и задаст необходимые вопросы. Волосы: <A> — расчесывали, <D> — стригли, <G> — заплетали, <J> — красили, <M> — мыли, <P> — жгли, <T> — какие были волосы, <AD> — другое. Ответьте буквой, соответствующей подходящему варианту, например (если во сне волосы стригли): D. После получения достаточной информации о Вашем сне Сонник пришлет Вам SMS с его трактовкой.

Особо суеверные абоненты очень любят присматриваться к окружающим черным кошкам, поминутно долбить деревянные предметы и внимательно слушать карканье ворон. Теперь в этом нет никакой необходимости: все будет понятно и без длительных и чрезмерно сложных упражнений — чтобы понять окружающие приметы и истолковать их должным образом, надо включить услугу PRIMETA (отправить SMS на номер 684) и выбрать описание предмета, явления и события. После получения всех необходимых данных на сотовик придут несколько SMS с мыслями о том, как и что надо понимать.

Кстати, если замучитесь читать всякие знаки Зодиака, проще обратиться к идеальной модели будущего — китайскому гороскопу. Это древний восточный гороскоп, в котором характер человека определяется по году его рождения. Знаки в нем определяются годами так называемого циклического календаря, причем услуга «китайский гороскоп» может помочь вам по-новому взглянуть на свою судьбу. На все тот же 684 отправляете SMS следующего вида — CHINA 1972 M, где 1972 — год вашего рождения, а M — указание пола (M — мужчина, W — женщина). Дата и указание на пол отделяются пробелом. Ну, и потом сразу, без утомительного ожидания, получаете полный список своих характеристик и особенностей — одним словом, прелесть!

Абонентам МегаФона выпало более интересное зрелище. Помимо Зараева, есть еще прорицатели на земле русской — это тяжелая артиллерия, прогнозы которой постоянно сбываются. Позвонив по 6122, можно узнать свое будущее персонально из уст Павла Глобы! Заглянуть в свое будущее можно не просто «абы куда — все равно интересно», а строго по пунктам меню — на сегодня, на завтра, на предстоящую неделю, на текущий месяц, на этот год. Однако на этом гуру астрологии никак не останавливается — исходя из положения звезд, он предлагает свои медицинские рекомендации, толкование снов, приметы, рекомендации по правильной пище и наиболее адекватной одежде. Поскольку база обновляется регулярно, прогнозы всегда свежие — оригинальный продукт из первых рук, хорошего качества, всего за 60 центов в минуту. Недорого — и оптом, и в розницу.

Мобильные курьезы

Такие функциональные и вроде бы серьезные мобильные телефоны все-таки становятся объектами забавных случаев, вызывающих улыбку и пользователей.

К примеру, на Украине отпраздновали десятилетие мобильной связи метанием сотовых телефонов, где турниры прошли в семи городах страны — Харькове, Днепропетровске, Донецке, Симферополе, Одессе, Львове и Киеве. Соревнования проводились в два этапа: сначала городские состязания, затем — финальное состязание их победителей в Киеве. Городской рекорд был установлен в Харькове — 55 м (модель телефона, к сожалению, не известна). Чтобы поставить

участников финала в равные условия, всем им выдали по телефону Samsung SGH-C100. Для оценки результатов соревнований была приглашена спортивная судейская коллегия международного класса. Интересно отметить, что большинство участвовавших в соревнованиях аппаратов сохранили свою работоспособность. Звание рекордсмена досталось 41-летнему киевлянину, который метнул свой мобильный телефон Motorola Starteck на 93 метра, что превысило официально зарегистрированный мировой рекорд. В качестве приза победитель получил мобильный телефон элит-класса Samsung V-200. Официально зарегистрированный мировой рекорд по метанию мобильных телефонов, установленный на чемпионате в Финляндии в августе 2002 года, составил 66,2 м. В сентябре 2002 года во Львове был поставлен рекорд 82,86 м.

А южнокорейский сотовый оператор SK Telecom не стал ломать современные модели сотовиков у своих абонентов, а, наоборот, предложил им очень полезный, но необычный сервис — специальную мелодию для мобильников, отпугивающую кровососущих насекомых. В Корее недавно начался сезон дождей, и в этот период, как правило, количество комаров значительно возрастает. При этом корейские комары не только надоедливы, но и чрезвычайно опасны для здоровья: они являются переносчиками тяжелых заболеваний, в частности, малярии. Мелодии для мобильников, отпугивающие насекомых, практически не слышны для человеческого уха. Эти мелодии звучат постоянно и отпугивают комаров и других насекомых в радиусе примерно одного метра. Во время испытаний, проводившихся в SK Telecom, мелодии отпугивали комаров достаточно эффективно. Стоимость загрузки противомоскитной мелодии в телефон составляет примерно

2,45 доллара США. Отрицательным моментом использования для борьбы с комарами специальных мелодий звонка является значительное сокращение времени работы телефона от батарей. С постоянно включенным отпугивателем москитов средний аппарат работает без подзарядки не более пяти часов. То есть использовать телефон для борьбы с комарами вдали от электрической сети не следует. В таких случаях больше подходят традиционные средства. Следует напомнить, что еще в 2001 году в Таиланде была написана компьютерная программа, генерирующая звуки, отпугивающие насекомых.

В России комаров пока не так много, и есть шутки поинтереснее — в московской сети МегаФон SMS теперь умеет говорить человеческим голосом — абонент «МегаФона» может написать SMS любого содержания (например, стихи или поздравление с праздником) и, указав в тексте сообщения телефонный номер адресата, отправить SMS-послание на короткий номер 000760. Адресат получит звонок и, сняв трубку, услышит «телегу» — сообщение будет прочитано человеческим голосом! Отправитель может выбирать для исполнения «телеги» любые голоса — мужские и женские, разного тембра, а также время доставки звонка. Особенной популярностью пользуется сообщение «Мы следим за каждым твоим шагом» или «Рота, подъем!» в исполнении строго мужского голоса. Кроме того, можно отправить сообщение в виде уже готового текста — на сайте www.telega.ru собрана целая коллекция анекдотов, телефонных приколов, веселых автоответчиков, тостов, поздравлений и т. д. И, наконец, самое главное — отправить голосовую «телегу» по SMS можно на любой телефонный номер, не обязательно мобильный, — на домашний, рабочий, по межгороду и так далее.

Стоимость одного сообщения составляет всего 40 центов — совсем недорого за возможность увидеть улыбку на лице знакомого человека.

А в Японии молодые пользователи сотовых телефонов так расшалились, что невинные забавы приняли характер массового бедствия — книжные магазины Японии планируют начать в стране кампанию по запрету так называемых «цифровых краж», осуществляемых покупателями с фотокамерами в мобильных телефонах. Японская ассоциация издателей журналов заявляет, что такая практика является кражей информации, и ей надо положить конец. Однако большинство молодых японок о таких вещах совершенно не задумывается. Увидев в глянцевом журнале новую прическу или одежду и желая узнать мнение подруг, они просто фотографируют страничку встроенной в телефон камерой и пересылают в электронном виде. Издатели этих журналов, соответственно, считают, что в результате у них падают продажи. На пару с японскими операторами сотовой связи они расклеивают суровые плакаты, напоминающие покупателям о правильных «журнальных манерах». К тому же, владельцы магазинов говорят, что их сотрудники не могут с уверенностью сказать, когда покупатель просто говорит по телефону, а когда делает снимки.

Распространение мобильных телефонов настолько сильно повлияло на этот мир, что детям теперь никак не получится разыграть своих родителей — специалисты из компании BlueTag создали технологию, позволяющую родителям расслабиться во время отдыха (в данном случае в зоопарке), а при необходимости даже забыть о своих чадах. Всегда знать, где находятся дети, позволят BodyTags — миниатюрные передатчики Bluetooth, прикрепленные к одежде малышей.

Местоположение детей устанавливается с помощью беспроводной LAN. При входе в зоопарк родители должны будут регистрировать в системе свои мобильники, а затем спокойно гулять по аллеям и рассматривать животных. Если они по какой-то причине потеряют из виду своего ребенка, то могут послать по сообщенному им адресу запрос по SMS, и через 20 секунд после отправки сообщения получат ответ — точную информацию о том, где находится их чадо. К тому же, при перемещении детей из одной части зоопарка в другую их родители будут автоматически получать на свои мобильники SMS-сообщение. Испытания новой системы слежения должны начаться в июле 2003 г. в Дании. В распоряжении руководства Ольборгского зоопарка находятся 200 меток и 50 точек доступа.

Не повезло жителям туманного Альбиона. Точнее, той части жителей, которая будет сдавать экзамены — в учебных заведениях Великобритании появятся детекторы мобильных телефонов. Поскольку в последнее время участились случаи, когда студенты на экзаменах используют мобильники (в том числе и с доступом в Интернет), чтобы получать ответы на вопросы по электронной почте или SMS, было принято не считать это больше невинными шалостями, а принять строгие меры. Ведь дети дошли до того, что используют встроенные в мобильники камеры, чтобы фотографировать экзаменационные работы и получать ответы! Появились даже специальные веб-страницы с вариантами ответов на билеты. В этом году попалось уже 360 студентов, причем в некоторых случаях выяснялось, что студентам подсказывали их собственные родители. В этой связи министерство образования делает ставку на установку в аудиториях специальных сканеров, которые обнару-

живают любой работающий мобильный телефон. Один такой сканер стоит примерно 200 фунтов стерлингов. А успешное тестирование сканеры прошли в школе Heathland School в Лондоне — контролеры обнаружили включенные мобильники в экзаменационных аудиториях и в библиотеке, где пользование телефонами запрещено. На первый раз детишек пожурили, но ведь могут и выгнать. Хотя самое лучшее — устанавливать глушилки мобильных телефонов, — тогда совсем никакой связи не будет.

А вот в Поднебесной творится просто ужас — хоть стой, хоть падай. Оказывается, не всякая атипичная пневмония или иная зараза, а злоупотребление SMS в Китае стало угрозой для здоровья пользователей. Огромная популярность в Китае передаваемых через мобильные телефоны коротких текстовых сообщений (SMS) начала приводить к травматизму среди поклонников этого средства общения — в результате злоупотребления SMS ряд пользователей были вынуждены обратиться за медицинской помощью в связи с повреждением связок большого пальца, которым производится набор текста на клавиатуре телефона. Доктора Народной больницы провинции Ганьсу, которые впервые столкнулись с такими пациентами, рекомендуют воздерживаться от чрезмерно активного использования SMS, поскольку слишком частая и быстрая работа с маленькой клавиатурой мобильного телефона действительно может приводить к излишнему напряжению кистей рук и повреждению больших пальцев. В 2002 году через сети основных китайских операторов мобильной связи China Mobile и China Unicom было передано около 90 млрд. коротких текстовых сообщений — в среднем 246 млн. в сутки. В период вспышки атипичной пневмонии (SARS) среднесуточное

количество SMS, передаваемых по этим сетям, достигало 300 млн.

Мобильные викторины

Проверяли ли Вы когда-нибудь свои знания? Тесты, опросы, контрольные, всевозможные конкурсные испытания — как в этот момент хотелось все бросить и уйти! А с другой стороны, было жаль, что под рукой нет шпаргалок, или заранее невозможно было потренироваться, чтобы показать гораздо более выигрышные результаты. Однако с появлением мобильных телефонов обе эти возможности становятся вполне осуществимыми — правда, тренинговых сервисов гораздо больше, чем всех остальных, вместе взятых.

Хотите проверить эрудицию? Попробовать правильно ответить на пару десятков вопросов и ни разу не споткнуться о сложную тему? Если да, то стоит обратить внимание на сервисы БиЛайн — викторин здесь видимо-невидимо. Есть простые викторины, есть викторины о народных приметах, есть обыкновенные викторины (вопрос-ответ) и есть образовательные викторины. На сайте www.beeonline.ru можно просмотреть список с описанием и выбрать себе забаву по душе. После этого надо отправить по sms на короткий номер 684 название викторины, например: VL. Получив сообщение с вопросом викторины, отвечайте буквами из угловых скобок, соответствующими правильному варианту ответа. Например, получив: Какой системы печка была у Емели?: <A> — буржуйка, <D> — русская, <G> — микроволновка, — отправьте в ответ: D. Ответив правильно, Вы получите следующий воп-

рос, при неправильном ответе — правильный ответ и буквы, которыми следует ответить для продолжения викторины.

Особо следует отметить образовательные викторины — они кроме краткого правильного ответа дают развернутое объяснение. Чего стоит VOA — викторина про амулеты, которая расскажет о том, какая детская игрушка обязательно нужна ребенку как средство от нечисти, что нужно носить в качестве талисмана на шее в ладанке, чтобы начальство на работе было благосклонным, или какой талисман, сделанный из впервые в жизни пойманной рыбы, поможет рыболову. Также впечатлила VOII об истории искусства — узнал, наконец, кто расписал потолок Сикстинской капеллы, когда Москву стали называть «белокаменной» и какое направление разрабатывал Сальвадор Дали. А VONOZH о холодном оружии оказалось очень близкой мне темой. Сразу отгадал, каков вес сабли, какое оружие можно надеть на голову и какое оружие было проклято Папой Римским. Студентам и школьникам рекомендую также викторины VOIST (история), VOISK (искусство), VOANIMAL (биология), VOGEOL (геология), VOLING (лингвистика), VORAST (викторина о различных видах флоры), VOLIT (литература). Полученные и актуализированные в результате общения с умным компьютером знания обеспечат хорошее отношение экзаменаторов и правильные ответы на зачетах и экзаменах.

Можно отвечать на вопросы одной викторины в течение несколько дней, система помнит уже заданные вопросы. Для того чтобы начать викторину с начала (забыть заданные вопросы), отправьте на 684 имя викторины с опцией — С (не забудьте пробел). Никакой дополнительной платы за игру не взимается, вы оплачиваете только стоимость исходящих SMS-сообщений согласно вашему

тарифному плану.

Компания МегаФон пошла чуть дальше в желании помочь абитуриентам, студентам и школьникам подготовиться к жестоким вступительным и выпускным экзаменам — на WAP-сайте столичной сети «МегаФон» wap.megawap.ru появился очень полезный раздел — «Студенту». Здесь собрана и систематизирована справочная информация по следующим предметам: русский язык (основные правила грамматики), математика (базовые формулы), физика (законы и базовые формулы). Воспользоваться новой услугой предельно просто: достаточно загрузить WAP-сайт, и нужная информация будет найдена очень быстро, в несколько «кликов», при помощи удобного рубрикатора. Одна особенность — использовать эти прелести цивилизации смогут только абоненты компании МегаФон.

Удобная новинка от «МегаФона» поможет студентам и учащимся старших классов не только с формулами и правилами, но и с вычислениями. WAP-калькулятор, специальное приложение к «Студенту», умеет вычислять тригонометрические и логарифмические функции, которые невозможно вывести при помощи обычного, встроенного в мобильный телефон, калькулятора. Кстати, если у пользователя будет MMS-телефон, то все формулы и данные будут представлены в цвете. Кроме того, к услугам пользователей — англо-русский и русско-английский «Переводчик» и рубрика для полиглотов «Энциклопедия», где можно найти справку по самым разнообразным темам — от компьютеров до кулинарии. Причем настроить показ нужных формул и правил можно в индивидуальном режиме — не надо «бегать» по всем разделам сайта, теряя драгоценное время. С помощью обычных настроек, доступных любому пользователю, надо про-

сто создать собственную WAP-страницу с любыми записями и «шпаргалками», которые будут доступны только владельцу конкретного сотового телефона и могут быть выведены на дисплей в течение нескольких секунд.

МТС в этом отношении немного отстает от своих конкурентов. Самое интересное, что могут предложить — это «Интересные факты». Самые интересные и занимательные факты из всех областей науки можно увидеть прямо на дисплее своего сотового телефона. Воспользуйтесь «Интересными фактами», и Вы узнаете ответы на множество вопросов, познакомитесь с секретами и тайнами нашего удивительного мира. В общем, с помощью этой мини-энциклопедии можно подготовиться к ответу на уроке или семинару — есть темы про государство, космос, знаменитых современников, природу, недра, транспорт. Короткий номер для отправки запросов — 1017. Формат запроса очень прост — <N> — запрос интересного факта под номером N (номера с 1 до 1010), <тема> — запрос интересного факта по теме. А чтобы получить факт на русском языке (по умолчанию — на транслите), добавьте в запрос после Темы <R>.

А для людей, сдающих языковые тесты, будет незаменим Мобильный sms-переводчик (только не забудьте перевести телефон в режим вибровызова!). Услуга «Мобильный переводчик» (номер 1020) позволяет оперативно перевести необходимое слово с русского языка на английский язык и обратно при помощи мобильного телефона. При отправке переводимого слова на короткий номер «1020» система автоматически распознает, на каком языке прислано слово, и в соответствии с этим переводит его на английский или русский язык. Ввод слова на русском языке возможен как в транслитерации, так и в кириллице (для тех моделей сото-

вых телефонов, которые поддерживают ввод текста кириллицей). Если русское слово в транслитерации совпадает в написании с английским словом, система присылает варианты русско-английского и англо-русского перевода. Таким образом, мобильный телефон превращается в очень удобный, воистину карманный переводчик с огромной базой слов!

Никакой дополнительной платы за указанные сервисы не взимается, вы оплачиваете только стоимость исходящих SMS-сообщений согласно вашему тарифному плану.

Сотовая связь: что дальше?

Совсем недавно европейское агентство Ananova привело любопытные результаты статистического исследования среди британских абонентов мобильных сетей в возрасте от 15 до 35 лет. Оказывается, почти три четверти англичан предпочли бы потерять бумажник, чем мобильный телефон. 72% опрошенных буквально помешано на мобилах, а 86% чувствуют себя без телефона как без рук. 23% меняют вызывной сигнал каждую неделю. Любопытно, что три четверти абонентов прибегали к использованию SMS, когда хотели избежать трудной беседы (вот он — источник популярности коротких сообщений!). Для подростков и молодежи портативные телефоны достигли статуса культа. И дело не в том, что по телефону можно говорить отовсюду, важно то, что телефон говорит о своем владельце.

В наше время трудно делать прогнозы — обычные инженерные проекты далеко опережают самые смелые мечты писателей-фантастов. Поэтому не будем забираться в дебри

«светлого будущего», а просто попытаемся заглянуть в чертежи разработчиков мобильной техники завтрашнего дня.

Сотовый телефон, как средство связи, вероятно, уже достиг своего совершенства. Прекрасные и легкие телефоны, в которые встроены sms, ems, gprs, wap и подобные прелести, стали стандартом. Они доступны по цене, просты в обслуживании и эксплуатации. Увеличение размеров зоны обслуживания и снижение стоимости разговора — вопрос, в общем-то, не столько технический, сколько организационный. Интересно другое: использование цифровых технологий для передачи данных открывает широкие перспективы для «нетрадиционного» использования телефона.

Первое, что приходит в голову и уже осуществляется, — совмещение функций сотового телефона и электронной почты. Два-три раза в день проверить свой почтовый ящик нетрудно, но среди обычных электронных писем частенько попадаются и такие, на которые стоило бы ответить немедленно. Если телефон будет способен принимать письма с пометкой «срочно» и даст возможность ответить на такое сообщение немедленно, то на сэкономленные деньги (от вовремя заключенной сделки или непотерянного клиента) можно будет приобрести «мобильники» всем членам моей семьи, включая домашнего йоркширского терьера. «В нагрузку» можно еще добавить к сотовому телефону функции пейджера, подключив свой номер через абонентскую службу пейджингового оператора, и пользователь теперь постоянно доступен для получения информации.

Точное местоположение — основа успешного ведения дел и прекрасных впечатлений от отпуска. Многие сотовые операторы уже предлагают использовать специальную функцию в модифицированных sim-картах под названием «Ближай-

шие» — с помощью своих станций они определяют местоположение пользователя и указывают ему необходимые рекомендации по маршруту следования или наличию тех или иных предприятий поблизости. Однако, чтобы быть автономным, да и еще и контролировать несмышленых детей, лучше воспользоваться несложной приставкой на основе спутниковой системы определения координат (GPS-локатор), которая вполне могла бы внести некоторое спокойствие в души сомневающихся родителей. Нечто подобное предлагает фирма Nokia для своих коммуникаторов 92xx. Процедура «превращения» довольно проста — достаточно подсоединить к смартфону специальный модуль LAM-1, содержащий в себе GPS-приемник и интегрированную антенну (подключение внешней антенны тоже допускается). Легкий модуль (вес всего 30 граммов) соединяется с коммуникатором через стандартные разъемы и питается тоже от него. Если учесть, что при работе GPS-приемник потребляет около 50 мА, а в ждущем режиме менее 1 мА, заряда аккумулятора смартфона хватит более чем на 5 часов полноценной навигации по городам и весям. В комплекте с LAM-1 прилагаются 2 CD-ROM с фирменным программным обеспечением TomTom CityMaps и RoutePlanner, внешняя GPS-антенна и чехол для хранения модуля. Программное обеспечение от TomTom рассчитано на топографию Западной и Восточной Европы, в базу программы CityMaps занесены более чем 100 000 городов таких стран, как Австрия, Бельгия, Дания, Франция, Германия, Англия, Италия, Люксембург, Нидерланды, Португалия, Испания, Швеция и Швейцария (России, к сожалению, нет).

А полиция Бостона, США, проводит испытание новой технологии, которая направлена на борьбу с теми, кто прогуливает занятия в школе. 65 полицейских получили мобильные

телефоны Motorola i85 с внедренной технологией, разработанной компанией NexTel Communications. В случае, если полицейский обнаружит подростка на улице в учебное время, он может получить на мобильный телефон расписание школьника и узнать, таким образом, прогуливает ли тинейджер школу. Новая технология позволяет полицейским получать на мобильный телефон информацию о расписании каждого из 63 тысяч школьников города. Раньше полицейским приходилось иметь при себе толстую книгу с расписаниями и информацией о каждом ученике. Новая технология позволит не только идентифицировать прогульщика, но и, получив данные о родителях ученика, отправить им сообщение на мобильный телефон.

Если добавить к GPS-приемнику кнопку экстренного вызова милиции или службы безопасности фирмы, прогулки по ночному городу могут быть просто приятным приключением, а не испытанием неверной судьбы. Особенно это полезно, если в стоимость услуги входит не просто оповещение «органов» об экстремальной ситуации, но и вызов на место оперативной группы с автоматическим оружием.

Если проставить на сотовый телефон датчики открывания дверей автомобиля — получаем весьма надежную противоугонную систему для автомобиля. Система может быть многофункциональной — при установке в автомобиль следящих систем при угоне автомобильный компьютер сможет выдавать на сотовый телефон владельца информацию о скорости, направлении движения автомобиля, дублировать эту информацию на компьютеры полиции. В таком случае у угонщиков не будет никаких шансов. При весьма миниатюрных размерах современных мобильных телефонов они вполне могут выдержать такую «операцию» — в таком случае, сво-

бодного места в карманах прибавляется. Да и потеря столь важного устройства в пределах дома, как это обычно случается в самый важный момент, практически исключена — ведь чтобы найти оснащенный такими функциями сотовик, надо просто на него позвонить и идти на звук.

Нетрадиционное использование новых функций gprs и, в будущем, 3G — подключение мобильноготелефона к сети Интернет с целью превращения его в великолепный цифровой «радиоприемник» с доступом к десяткам тысяч радиостанций во всем мире. Телефоны с FM-приемником существуют, но это, право, скучновато — слушать только радиостанции своего города. Ведь многие зарубежные станции вещают в сети Интернет — и слушать их можно за относительно небольшие деньги, которые надо будет платить только за трафик. Зато преимущества очевидны — стереовещание с высоким качеством, произвольный выбор любого из тысяч каналов, автоматический перевод на основные языки. При совмещении приемника с цифровым магнитофоном появляется возможность слушать записи в стандарте MP3, использовать приемник как диктофон или записывать понравившиеся радиопередачи.

С таким аппаратом точно не захочется расставаться. Именно для таких фанатов-пользоваетелей два инженера, проживающих в Великобритании, создали зубной имплантант, способный выполнять функции мобильного телефона. «Зубной телефон» сейчас состоит из крохотного вибратора и приемника радиоволн. Он будет вживляться прямо в зуб в ходе обычного визита к стоматологу. Звук поступает в зуб с помощью цифрового радиосигнала, который затем путем костного резонанса передается во внутреннее ухо. Информация, передаваемая таким образом, слышна только одному человеку —

тому, кому она адресована, так что пользоваться «зубным телефоном» можно в любом месте и в любое время. Это делает новинку особенно привлекательной для политиков, которые смогут полностью конфиденциально слушать советы своих помощников во время публичных выступлений, и для биржевых брокеров, которые таким образом смогут получать информацию, касающуюся акций. Удобны «зубные телефоны» и в повседневной жизни — их не нужно отключать в кинотеатрах и музеях. Технология сейчас проходит испытания, и телефон приобретет свой окончательный вид уже в ближайшее время. Так что, по мнению изобретателей, «зубной телефон» имеет все шансы стать первым гаджетом, целиком вживленным в человеческое тело и способным при этом работать без вспомогательных устройств.

Еще одно нетрадиционное использование сотового телефона — как средство самообороны. В телефон можно встроить пистолет на два-четыре патрона 22 калибра. Современные модели таких телефонов созданы, в основном, для камуфляжа оружия и служат им как футляр, в будущем имеет смысл достигать совмещения этих функций. Чтобы зарядить такой пистолет, нужно будет сдвинуть в сторону половинку корпуса телефона. Патроны 22-го калибра вставляются в верхнюю часть корпуса под дисплеем. В нижней части расположены контакты, соприкасающиеся с капсюлями. Достаточно на клавиатуре нажать цифры 5, 6, 7 или 8, как раздастся выстрел. Пули вылетают через отверстие в антенне.

Еще одна современная тенденция — создание телефонов с отделениями для нескольких sim-карт и с возможностью работы через спутник при отсутствии зоны покрытия сотовой сети. Стационарные же сотовые устройства (язык не поворачивается назвать эту штуку телефоном) смогут обес-

печить телефонную связь и выход в Интернет из любого частного дома, коттеджа или автомобиля, не обращая внимания на пресловутое «кабелирование». Пройдет еще несколько лет, и человек без «мобильника» будет выглядеть очень странно.

Взрывающиеся мобильники

Совсем недавно исследовательская компания Forrester Research заявила очевидную, по большому счету, вещь — чем шире распространяются мобильные телефоны, тем чаще люди отказываются от аппаратов фиксированной связи. В этом есть свои плюсы и минусы. Основные проблемы возникают с тем, что мобильные телефоны становятся очень значимыми в жизни современных городских жителей — их чаще крадут, они чаще выходят из строя, и потеря времени на ликвидацию мелких технических проблем растет. Появляются и новые опасности, одна из которых — потенциальная взрывоопасность мобильных телефонов. Еще несколько лет назад в это невозможно было поверить, однако сейчас — это действующие реалии.

Взорваться современные мобильные телефоны могут в трех случаях: во-первых, созданы новые механизмы для защиты мобильных телефонов при краже. Ученые Калифорнийского университета случайно нашли возможное решение проблемы воровства сотовых телефонов, карманных компьютеров, цифровых камер и других устройств, основанных на применении кремниевых микросхем, сообщает английская газета The Guardian. Один из сотрудников профессора Майкла Сейлора столкнулся с ситуацией из филь-

ма «Миссия невыполнима» (помните, «Это сообщение будет уничтожено через 10 секунд»?), когда попытался разбить кремниевый чип, обработанный нитратом гадолиния (редкоземельный металл, элемент №64), — в результате прогремел взрыв. По словам ученого, это было похоже на удар по пистону с последующим воспламенением. Такой эффект может вызвать электронный сигнал, поступивший от владельца украденного устройства, или неправильное вскрытие телефона, например, для замены SIM-карты. Взрыв не настолько силен, чтобы причинить серьезный вред похитителю, но вполне достаточен, чтобы уничтожить само устройство. Чип также может быть применен и в стационарных компьютерах для защиты секретных данных. Способность пористого кремния абсорбировать из окружающей среды определенные элементы дает возможность использовать этот материал в качестве детектора для обнаружения в воздухе опасных газов и биологически вредных веществ.

Хотя стоит знать несколько простых правил, прежде чем взрывать свой сотовый телефон при краже. Позаботиться о безопасности можно сразу же при покупке, застраховав телефон на случай кражи, потери или пожара. При потере прежде всего обязательно сообщить оператору о пропаже — для блокировки счета с деньгами. Эта услуга обычно бесплатна. Также стоит позвонить на пропавший телефон, и если он лежит в такси или в каком-нибудь людном месте, то шанс получить его обратно еще не упущен. Еще один вариант — установить персональный код, который будет запрашиваться после каждого включения. Правда, это действует только на неопытных взломщиков.

Во-вторых, сотовый телефон может быть вполне реальной бомбой и взорваться в результате террористического акта

или работы специальных служб. В ходе арабо-израильского конфликта в 2002 г. противоборствующие стороны активно использовали бомбы в мобильных телефонах — специальные службы таким образом ликвидировали террористов, пряча 50–60 грамм взрывчатки в корпус аппарата, а террористы дистанцировались от мест проведения взрывов, используя мобильный телефон как передатчик радиосигнала для активации детонатора взрывного устройства. А в разгар криминальных войн в Москве в середине 90-х от звонка «мобильника» взрывались самодельные бомбы.

Пострадать от взрыва телефона с взрывчаткой в корпусе почти невозможно — он поражает только голову абонента и является взрывным устройством направленного действия. Распознать его можно в основном по весу — телефон с пластиковым зарядом внутри тяжелее аналогичных аппаратов той же модели. Может насторожить некоторый специфический запах трубки или утяжеление (визуальное увеличение) отдельных частей телефона — антенны, толщины аппарата, кнопок и т. д.

В-третьих, сотовый телефон может взорваться от действия новых видов топлива. Не секрет, что ученые, в своем желании изменить мир к лучшему, собираются многие устройства, традиционно питающиеся от электроэнергии, перевести на газовое топливо. Компания Motorola объявила о том, что приступила к разработке принципиально нового средства питания для своих телефонов и ноутбуков — миниатюрного топливного бака. Сообщается, что уже удалось создать специальную многоуровневую систему, в которой газовое топливо смешивается с воздухом, после чего подается на электронный мембранный узел. При комнатной температуре результатом смешивания газа и кислорода является вырабатывае-

мая электроэнергия. Так что в скором времени свет увидит первая питательная батарея, представляющая собой нечто среднее между традиционной батареей и топливным баком. Единственное, что остается главной сложностью специалистов, — обеспечение такого уровня безопасности, при котором взрыв топливного бака был бы невозможен даже теоретически. Не очень приятно, согласитесь, если мобильник взорвется в вашей руке во время разговора, и его счастливый обладатель останется без головы! К сожалению, примеры взрыва топлива общеизвестны. Один из самых трагичных — взрыв топливного бака реактивного самолета Конкорд во французском аэропорту. Так что перед тем, как оснащать современные устройства новым типом питания, потребуется проделать еще немало работы. Но факт остается фактом — скоро на газе будут работать даже сотовые телефоны. Уберечься от такого взрыва пока очень легко — не стоит проверять на себе экспериментальные образцы топлива будущего — лучше уж старые добрые электрические аккумуляторы.

Вообще сотовые телефоны в современном мире — вполне опасная вещь, если использовать их с нарушением инструкции. Сами мобильники внушают людям некоторую опасность из-за мифов об опасности электромагнитных лучей — но это проблема не медицинская, а психологическая. Мы не видим электромагнитных лучей, не слышим их, не ощущаем. Они недоступны нашим чувствам, и именно это сеет в людях страхи. На самом деле, ничего страшного в мобильных телефонах нет. Большинство из них работает в диапазонах 900/1800 МГц. Нашему здоровью это не вредит. Куда опаснее, если человек, звоня по «мобильнику», забывает, где он и что он делает. По данным журнала «New England Journal of Medicine», у водителей, пользующихся телефоном, шансы

попасть в аварию в четыре раза выше, чем у тех, кто смотрит на дорогу. Стоит всего на секунду отвлечься, разогнавшись до 100 километров в час, и ваша машина будет ехать вслепую 20 метров. Известны случаи, когда в самолете срабатывала пожарная тревога только из-за того, что пассажиры звонили в опасной близости от сигнализации. Электромагнитные волны, излучаемые телефоном, могут сказаться и на работе других приборов, ведь самолет напичкан электроникой. Так, они могут глушить радиосигналы наземных станций слежения. Порой нарушается режим работы домашних приборов, например, стиральной машины. «Мобильник» срабатывает как пульт. Случайный звонок может вывести из строя искусственный стимулятор сердца, переключить больничную автоматику и даже снизить температуру в инкубаторе для новорожденных.

Впрочем, все эти инциденты очень редки. Сотни миллионов жителей нашей планеты спокойно пользуются «мобильниками» без всяких последствий для окружающих. Тысячи авиапассажиров болтают по телефону в салоне самолета — и тоже без вреда. Однако по мере того, как мобильные телефоны все настойчивее входят в нашу жизнь, количество подобных казусов — и безобидных, и неприятных — будет все нарастать.

Вопросы безопасности

Фальшивый prepaid

Подделка, как форма мошенничества, стара как мир. Сначала подделывали банковские карты, потом карты таксофонные, потом карточки для доступа в Интернет, сейчас — карты предоплаты за сотовую связь. Как оказывается — дело выгодное.

Еще в 2002 году управление «Р» МВД РФ задержало продавцов фальшивых карточек — злоумышленники взломали сервер компании «Дитжитал Нетворк» и получили несанкционированный доступ к программе изготовления платежных карт, дающих право доступа в Интернет. В ходе контрольной закупки студент 4-го курса МИФИ продал милиционерам за $60 фальшивый номер платежной карты, по которому предоставлялся доступ на сумму $100. Вскоре был задержан и сам организатор преступления. При обысках у задержанных изъяли компьютерную технику, носители

информации и возбудили уголовное дело по статье 272 УК РФ (неправомерный доступ к компьютерной информации).

Отдельный бизнес — подделка телефонных карточек. В последнее время участились подделки таксофонных карточек с памятью — для этого необязательно изготавливать непосредственно фальшивую карточку. Подделка может состоять в том, что создается специальное устройство, которое отвечает на запросы таксофона так же, как и легальная таксофонная карточка. При обнулении счетчика кредитов на такой мошеннической карте он автоматически восстанавливается до первоначального значения. Ясно, что компании-операторы терпят огромные убытки от мошенничества, особенно если фальшивая таксофонная карточка используется для междугородних и международных переговоров. Любой тираж таксофонных карточек изготавливается под конкретного оператора, т. е. при подаче питания на микросхему последняя отвечает таксофону уникальной последовательностью байтов, характерных для данного производителя карточки и таксофонного оператора. Тем не менее, уровень мошенничества с таксофонными карточками остается весьма высоким. Поэтому компании-производители таксофонных карточек постепенно переходят к производству их нового поколения, основанного на различных версиях новых чипов, где процесс аутентификации карточки построен на использовании секретных ключей, известных только эмитенту карточки.

Более «свежий» пример надолго запомнится многим участникам рынка сотовой связи — в начале мая 2003 г. разгорелся скандал с фальшивыми карточками предоплаты «Би Плюс». Как оказалось, дилер Вымпелкома компания «Станиоль» произвела гигантскую партию фальшивых карточек для пополнения баланса «Би Плюс», сумела продать своим парт-

нерам большую ее часть, а затем бесследно исчезла. А у столичных дилеров сотовой связи остались неработающие карточки «Би Плюс» примерно на четыре миллиона долларов, сообщают «Ведомости». По свидетельству пострадавших, всего на рынок было выброшено около 600 тысяч поддельных карт «Би Плюс» самого популярного номинала, по 10 и 20 долларов. ЗАО «Станиоль» небольшая, но хорошо известная компания, занимавшая примерно один процент столичного рынка. Именно поэтому «Станиоли» удалось в течение одного-двух дней продать по предоплате карточки на четыре миллиона долларов, — ведь ей доверяли. Также мошенники взяли под залог части карточек банковский кредит и с тем скрылись. Распродаже фальшивых карточек помешали именно «индивидуальные предложения». Крупным заказчикам давали скидку в шесть процентов, в то время как сам «Вымпелком» скидывает крупным дилерам только пять процентов. Когда «Станиоль» начала предлагать несусветные скидки, их сразу вычислили, — рассказал «Ведомостям» представитель одной из дилерских компаний. Однако результат налицо, и множество фирм понесли убытки. А вот абонентам, которые купили подделку, Вымпелком обещал деньги вернуть.

Подделка карточек — действие не очень сложное. На примере уже известных фактов подделки можно описать следующий способ: берется уже использованная карта (как правило, подделывают карточки большого достоинства), стертое поле с 14-значным номером заклеивается сигаретной фольгой, а сама карточка снова запаивается в полиэтилен. Теперь остается самое главное — «сдать» карточку. Реализация карточки не осуществляется самими мошенниками непосредственно клиенту — это опасно и хлопотно. Скорее всего, она попросту запускается в сеть продаж вместе с подлинными, а

там — лотерея. Как один из вероятных вариантов, представим себе следующий трюк: мошенник под видом покупателя подходит к месту альтернативной продажи карточек предоплаченного сервиса (киоск или лоток, но не специализированный салон) и покупает настоящую карточку. Передав кассиру деньги, он осуществляет подмену настоящей карточки фальшивой и ждет, когда, наконец, кассир сосчитает деньги и осчастливит его известием типа: «Здесь не хватает ста рублей!» После этого «раздосадованный» покупатель смущенно извиняется, озадаченно сводит на переносице брови, пытаясь понять, как это он «просчитался» в своей покупательской способности, и, вернув карточку, удаляется. Второй пример — подделка крупными партиями, как уже было описано выше. Суть в том, что изготавляются карты, внешне похожие на настоящие, степени защиты не особенно соблюдаются, так как рядовой потребитель и большинство продавцов об этом просто ничего не знают. Повторяются внешне все атрибуты настоящей карты, только вместо пин-кода пишется произвольное число знаков без всякого содержания. Рассчет на быстроту — сделка, получение денег/сдача товара и быстрый уход до тех пор, пока клиенты не начали жаловаться на невозможность пополнить баланс своего счета.

Меры безопасности, для того чтобы обезопасить себя от подделок, вполне разумны и очевидны:

1. Покупать карточки предоплаченного сервиса только в контролируемых дилерами местах (дилерских магазинах/салонах) — там пополнение счета, при желании, происходит при покупателе.

2. Если карточка по какой-либо причине приобретается не в специализированном салоне, то среди всех «альтернативных мест продажи» (все, что не есть салоны мобильной

связи) необходимо выбрать точку, работающую с любой известнейшей дилерской сетью и имеющую в своем наружном дизайне элементы символики этой сети — логотип, товарный знак и т. д.

3. При покупке в альтернативных местах продажи нужно проверять целостность упаковки.

4. Обратите внимание на защитное восковое поле: оно имеет волнистый рисунок.

5. При возникновении каких-либо трудностей с пополнением счета по купленной карточке тут же обращайтесь в сервисный центр оператора.

Механизм продажи услуг предоплаченного сервиса в специализированной сети от продажи в полулегальных источниках отличается подчас кардинально:

1. В сети продаж, контролируемой дилером, четко фиксируются номера карточек, по которым отслеживается их движение. Дилер по номеру карточки всегда сможет определить: была ли она продана через его сеть, когда и где она была продана в его сети, кем именно она была продана в его сети.

2. При возникновении каких-либо вопросов дилер имеет возможность оперировать достоверной информацией. Если это не позволяет найти ответ на возникшую у клиента проблему с пополнением счета, можно пойти дальше — обратиться к оператору в сервисном центре по номеру карточки — определить, когда и где был пополнен счет по этой карте.

Вывод очевиден: чтобы не услышать от консультанта сервисного центра неприятных известий о том, что карточка уже была кем-то использована или вообще фальшивая,

прочитайте наш материал внимательно и работайте только с дилерами. А еще лучше, платите только в кассах оператора — так надежнее.

Сотовые мошенничества

Неправомерное использование сотовых телефонов в преступных целях насчитывает небольшую, но очень бурную историю. Лавинообразная «мобилизация» населения не может оставить в стороне всякого рода мошенников, которые используют блага цивилизации в неблаговидных делах сомнительного качества.

По данным Международной ассоциации сотовой телефонии (CTIA — Cellular Telecommunications Industry Association), типовые потери западного и отечественных операторов составляют от 2 до 5%. По оценкам специалистов, общемировые потери операторов от мошенничества составляют 20–25 млрд USD в год. Однако стоит отметить, что профессионально сотовым мошенничеством в России занимаются немногие, их количество не выходит за допустимые рамки в 1–2% от клиентской базы оператора. Но тенденции показательны, и сотовое пиратство становится настоящей индустрией. По мнению экспертов, оно уже занимает первое место среди преступлений в сфере высоких технологий в крупных городах России.

Самые большие убытки сотовая компания может понести из-за мошенничества с использованием сотовых телефонов. Почти классический случай произошел недавно с отечественным GSM-оператором. Злоумышленники зарегистриро-

вали подставную компанию, арендовали платный номер в Европе и купили у российского оператора 50 телефонов, подключенных по кредитному тарифному плану. Затем они перевезли эти телефоны в Европу и поставили их на автодозвон до арендованного платного номера. Так они сгенерировали огромное количество очень дорогого трафика, приходящего на этот номер. В конце месяца FranceTelecom выплатил арендаторам номера несколько сотен тысяч долларов. Единственным пострадавшим от мошенников оказался сотовый оператор, которому французская компания выставила астрономические роуминговые счета — его ущерб составил около полумиллиона долларов.

Пользователям стоит осторожнее относиться к различного рода рекламе сомнительных услуг сотовой связи. Чистым мошенничеством являются призывы типа удвоения суммы на счете или организация фактически бесплатных (для оператора) разговоров. Реклама обычно отсылает на некоторый сайт в Интернет, где посетителям сайта предлагается подключиться к сотовой сети какого-либо оператора с «дополнительными услугами». Услуги же довольно специфичны: блокировка счета («Вы говорите, а деньги не снимаются», — поясняет реклама), система b2m («Вы переводите на наш счет какую-то сумму, а мы переводим на счет вашего мобильного номера сумму в 2 раза больше») и многое другое. Также на некоторых сайтах предлагается заказать «перепрошивку» программного обеспечения сотовых телефонов, позволяющую бесплатно делать некоторые виды звонков. Причем взломать предлагается сети не только столичных GSM-операторов, но и многих региональных и некоторых зарубежных. Однако стоит понимать, что это является совершенным вымыслом, единственная цель которого — выудить деньги у доверчивых

граждан. В случае любых проблем конечным звеном, которому придется иметь дело с компетентными органами, остается пользователь.

Также беспокоят экспертов подделки SIM-карт. Такая карточка, по размерам не больше ногтя, есть в каждом сотовом телефоне — здесь закодирована информация о пользователе и его телефонный номер. Если отклонировать sim-карту с помощью специальных технических устройств, то можно совершать дорогостоящие звонки от чужого имени, маскироваться в сотовых сетях и быть неуловимым абонентом. До недавнего времени проблема мошенничества почти не беспокоила компании, работающие в стандарте GSM. Считалось, что эта цифровая система, в отличие от других сотовых стандартов, на 100% защищена от высокотехнологичного мошенничества. Однако выросшая в сотни раз производительность компьютеров и наличие специальных программ, «разламывающих» криптографические системы, облегчила мошенникам задачу. Теперь с помощью «примочки», купленной на черном рынке меньше чем за 200 USD, и современного PC защита SIM-карт снимается за пару-тройку часов, а в случае с алгоритмом A5/1 (система шифрования информации, записанной на SIM-карты в GSM-сетях), как уверяют исследователи из Израиля, даже менее чем за секунду.

Надо отметить, что помимо телефонных номеров и коротких сообщений (SMS), SIM-карты хранят криптографические ключи, которые идентифицируют пользователя в GSM-сети, а также защищают передачу разговоров и данных от подслушивания или перехвата. Поэтому, по возможности, не передавайте свои SIM-карты в чужие руки, не раскрывайте персональные PIN-коды — даже близким людям. Печально, но мы беззащитны, так как на любой замок все-

гда находится отмычка, и передышки будут лишь в промежутках между разработкой замка и отмычки.

Платежи за мобильную связь — очень проблемная зона многих операторов связи. Для создания кода используется специальные алгоритмы генерации номеров, которые потом записываются в главную базу оператора. База по степени защищенности столь высока, что реально доступ к ней имеет только администратор, который тоже не может физически просмотреть эти номера. В базу данных встроена автономная система защиты, система проверки номеров на правильность и система контроля целостности самой системы (помимо множества других функций). Таким образом, оператор гарантирует себя от недобросовестных действий своего персонала, приближая безопасность своего финансового благополучия к стабильно высоким показателям. Если случается сбой, то база восстанавливается из резервной копии. В этом смысле есть очень интересные случаи с крупными отечественными операторами сотовой связи — происходили сбои в финансовой системе расчетов с абонентами, и абонентам можно было повторно активировать карту предоплаты, так как информация о том, что она уже действовала, была утрачена. При этом счет система исправно пополняла на сумму номинала. Однако такие приятные случаи бывали редкими, больше было событий в регионах, когда после сбоя абоненты получали на свои счета необоснованные списания денежных средств и астрономические задолженности, которые не соответствовали действительности и были возможны только из-за ошибок программного обеспечения операторов, когда меняли биллинговую систему.

Еще одно «узкое» место в данном случае — начисление денег на счет. Если это случай «барышня в киоске/кассе», то

степень защищенности передаваемых данных в центральный компьютер будет на высоком уровне — шифрование, идентификация, постоянные проверки платежей и наличности в кассе. Но это только в случае, если касса построена как официальный центр приема платежей какого-либо оператора. Подключиться к линии вряд ли удастся — во-первых, там используются не обычные телефонные кабели, а выделенные каналы связи, во-вторых, там стоит система, реагирующая на изменения уровня сигнала, что может свидетельствовать о несанкционированном подключении, в-третьих, линии связи защищены дополнительными специальными средствами, которые у каждого оператора свои, в-четвертых, надо знать коды доступа к самой подсети, коды терминала, куда идет соединение, ключи шифрования и передачи данных.

Однако есть и другой вариант — специальные автоматизированные терминалы (размером с книгу), которые торгуют пин-кодами за наличные. Схема подключения к центральному компьютеру проста — по обычной телефонной линии. Аппарат имеет модем, после подключения он авторизуется, вводя свои данные, и запрашивает у центрального компьютера пин-код с указанным номиналом (сумма зависит от натроек ПО — либо любая, либо четко фиксированная), который он печатает встроенным принтером и выдает покупателю вместе с чеком. Покупатель активирует пин-код так же, как и код, полученный на предоплаченной карте. Однако в этом устройстве, которые используются в странах СНГ, и кроются проблемы — связывается с центральным компьютером он по незащищенной линии, и перехватить данные можно элементарно — главное, активировать пин-код быстрее покупателя. Далее можно, но это потребует больше времени, понять данные, которые подобный

аппарат использует для авторизации с центральным компьютером, и попробовать эмулировать его работу, запрашивая любое количество кодов. Однако для этого нужны технические устройства и специальное оборудование.

Другое дело — предоплаченные карты. Есть множество ошибок в ПО (программное обеспечение) операторов — в частности, при пополнении счета по предоплаченным картам. К примеру, у некоторых операторов Украины систему биллинга можно обмануть, если одновременно с нескольких сотовых телефонов послать запрос на пополнение баланса по предоплаченной карте — то есть синхронно ввести код и нажать * по окончании ввода. Система считает, что это один пользователь, и если повезет, то на все участвовавшие в «процессе» телефоны система одновременно начислит сумму, равную номиналу карты. Такая же ошибка присутствует почти во всех системах, если обновление происходит через Интернет — открывается множество браузеров, в каждом из которых вводится пин-код, и все это надо быстро ввести нажатием клавиши Send. За счет «тормозов» в канале система воспринимает это одним большим пакетом. Иногда получается начислить себе на счет таким образом 5–6 лишних номиналов карты.

Мобильные телохранители

В будущем все изменят сотовые телефоны — с их помощью обеспечение личной безопасности станет более простым и менее опасным делом. Самое главное в любом процессе по охране человека — знать точное место расположения объекта

и возможность быстро прийти ему на помощь. Также важно вооружение — оно должно быть надежным и удобным для скрытого ношения. Со всеми этими проблемами предлагают справляться производители специализированных гаджетов и ПО.

Уже начат процесс внедрения телематических систем в работу современных телохранителей. Причем это не заокеанские новинки hi-tech, а самая, что ни на есть, отечественная действительность. Одним из первых опытов подобной интеграции является обеспечение безопасности визита Главы корпорации «Microsoft» Стивена Балмера в Москву Национальной ассоциацией телохранителей России. В период визита, который проходил в октябре, были использованы телефоны «ESC!» и «TRACK PRO» фирмы «BENEFON», подключенные к телематическому центру с программным обеспечением «Поиск-2», созданным компанией «ПРИН». Со своей задачей система справилась — сотрудники дежурной службы в любой момент знали, где находиться группа личной охраны. И всегда на карте местности отображалось местоположение каждого сотрудника. Система работает на основе SMS-сообщений оператора GSM-связи. Телефоны BENEFON снабжены приемниками GPS, с возможностью пересылки собственных координат по каналу GSM. Таким образом, дежурная служба отслеживала все передвижения перемещения каждого сотрудника личной охраны.

Телохранители Национальной ассоциациии телохранителей России, находящиеся в автомобилях, обеспечивающих встречу охраняемого лица в пункте прибытия, имели оперативную информацию о месте нахождения основной группы, скорости и направлении передвижения. И в любой момент были готовы либо выехать к месту происшествия или брать под охрану место прибытия. Анализ компьютерных данных

системы телематики позволил получить объективную картину объема работ, проведенных НАСТ России при подготовке и обеспечении визита Главы корпорации «MICROSOFT». Все перемещения автомобилей и сотрудников были отражены на компьютерных картах Москвы и Подмосковья. В заключение можно отметить удобство в использовании специализированных телефонов совместно с радиостанциями. Иметь возможность разговора с коллегой и при этом знать, где он находится в действительности, — это значительное расширение возможностей для тактических действий при обеспечении личной безопасности. И отличное средство для повышения персональной ответственности сотрудников.

Интересные устройства по защите тоже могут быть реализованы с помощью мобильного телефона — ведь стреляющий мобильный телефон или телефон-пистолет — идея, по-своему захватывающая. Внешне такие телефоны и сейчас, и в будущем очень схожи с обычным мобильником — они разве что тяжелее по весу, а в остальном — как вылитые. В особенности, если не держать в руках и смотреть издалека. Это не телефоны вовсе: ни с него, ни на него позвонить нельзя. По сути — это пушка в телефонном обличии. Перед стрельбой подобные устройства разделяются надвое: в верхнюю часть, то есть под дисплей, вставляются четыре патрона 22-го калибра. Потом оружие снова превращается в телефон, а в нижней части «телефона» оттягивается «как бы пружина». Патроны вставляются в четыре отдельные камеры, по капсюлям бьют четыре отдельных бойка, четыре патрона поочередно вылетают из четырех «стволов». И «курков» тоже четыре штуки — это кнопки для набора номера. Участвуют кнопки второго ряда: 4, 5, 6 и — главная «соединительная кнопка» — вероятно, «Send».

Однако пока существующие прототипы скорее для самозащиты — попасть во что-либо из них можно только с расстояния не более двух метров. В какой-то степени — это действительно существенный недостаток, но, с другой стороны, на то он и замаскирован под телефон — чтоб стрелять в упор. Однако есть и другие смертоносные игрушки закамуфлированные под сотовые телефоны — к примеру, устройство ShotCaller2000. Да-да, стреляющий телефон. В трубку закладывается один 9-миллиметровый патрон, который и сносит голову неприятелю после того, как получает отмашку в виде трехзначного кода с другого телефона.

А компания Micro-surveillance выпускает интересные изделия, которые хоть и не являются пистолетами, но считаются полноправными мобильными телефонами и одним из видов оружия одновременно. Micro-surveillance с 1989 года занимается разработкой и продажей всяческих средств обеспечения безопасности и шпионских штучек — микровидеокамер, крохотных передатчиков, устройств для самозащиты и тому подобного. И еще пример — 2002 XCellular Phone Type Stun Gun. Проще говоря — это мобильный телефон, совмещенный с электрошокером. Собственно, тут и говорить особо не о чем — бьешь хулиганов током, да и все — 120 тысяч вольт искрятся между антенной и неким шпенделем. Размеры аппарата — 150 Н 48 Н 30 мм, вес без батареи — 150 граммов. Стоимость — $145, но можно найти и дешевле.

Мобильная безопасность

Сотовые телефоны уже доступны по цене многим жителям нашей страны. Однако, как и в любом бизнесе, в телекоммуникационной отрасли существуют люди, готовые заниматься противоправными действиями. Мобильные телефоны могут прослушиватся для получения конфиденциальной информации, могут создаваться «двойники» с целью бесплатного пользования сотовой связью, могут взламываться пароли. Об этом надо знать, чтобы не стать жертвой преступных посягательств подобного рода.

На заре телекоммуникационного бума в России один питерский хакер изобрел занимательный способ прослушивания телефонов. Само устройство представляло собой самый обыкновенный модем, правда, несколько модифицированный. Устройство настолько универсально, что при помощи его можно было прослушивать и сотовую связь. Эти устройства можно было купить в Санкт-Петербурге по цене 5000 долларов за штуку, однако горе-изобретатель был пойман при передаче 30-ти своих устройств члену одной из преступных группировок. Но не стоит думать, что подобного рода происшествия целиком в прошлом.

Проблема безопасности при пользовании сотовым телефоном имеет два аспекта: физическая безопасность пользователя и безопасность информации, передаваемой с помощью этих устройств. 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. В настоящее время электронный перехват разговоров, ведущихся по сотовому или беспроводному радиотелефону, стал широко распространенным явлением. Электронный перехват сотовой связи не только легко осуществить, он, к тому же, не требует больших затрат на аппаратуру, и его почти невозможно обнаружить. Прослушивание и/или запись разговоров, ведущихся с помощью беспроводных средств связи, практикуют правоохранительные органы, частные детективы, промышленные шпионы, представители прессы, телефонные компании, компьютерные хакеры и т. п.

Для этой же цели можно использовать обычные сканеры после их небольшой модификации, которая, кстати, весьма подробно описана в Интернете, с включением в этот комплекс переносного ПК. Легче всего перехватываются неподвижные или стационарные сотовые телефоны, труднее — мобильные, так как перемещение абонента в процессе разговора сопровождается 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.

Такими же уязвимыми в отношении безопасности передаваемой информации являются и пейджеры. В большинстве своем 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 and 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 5000–10000 пейджеров одновременно и хранение всей переданной на них информации.

Также могут быть проблемы с использованием сотовых телефонов и у операторов — речь идет о мошенничестве. Мошенничество представляет собой постоянно развивающееся и многоликое явление. По мере перехода от аналоговых к цифровым системам (GSM) менялся характер мошенничества, поскольку нарушителям становилось все труднее (и, что более важно, дороже) перехватывать информацию и клонировать трубки. Однако полностью сбрасывать со счета возможность технического мошенничества в сетях GSM нельзя, так как если перед мошенником закрыта дверь, то он будет пытаться влезть в окно.

Подсчитано, что из-за мошенничества отрасль мобильной связи во всем мире теряет ежегодно около 25 млрд. долл., поэтому обнаружение, судебное преследование и предотвращение мошенничества так важно для всех операторов мобильной связи. Для решения этих задач в сетях GSM и будущих системах UMTS необходимо принимать дополнительные

меры безопасности, которые сделают их значительно менее уязвимыми.

Мошенничество — неправомочная деятельность, которая позволяет абонентам-нарушителям и хакерам получать услуги связи бесплатно. Компании иногда подсчитывают деньги, которые они теряют из-за мошенничества, определяя их как доходы, упущенные из-за неуплаты.

Хакерские мошенничества дают доход мошеннику за счет проникновения в незащищенную систему и использования (либо последующей продажи) имеющихся в системе функциональных возможностей. Примерами являются использование в целях мошенничества УАТС (местной АТС) и хакерское нападение на сеть (взлом сети). В случае мошенничества в УАТС мошенник многократно звонит в УАТС, стараясь получить доступ к внешней исходящей линии. Получив такой доступ, он затем может вести дорогостоящие телефонные разговоры, оплатив только недорогой звонок за доступ к УАТС. Зачастую такие звонки увязаны с использованием клонированных телефонов, так что не оплачивается даже использование недорогой местной линии. В случае нападения на сеть осуществляются атаки на компьютерные сети через линейные модемы, которые используются для дистанционного управления или контроля работоспособности внешних линий. После успешного проникновения в модем мошенник постарается взломать сеть и сконфигурировать некоторые системные параметры для собственных нужд. Такие виды мошенничества характеризуются (в тот период, когда хакер еще только пытается получить несанкционированный доступ к сети) либо частыми короткими звонками на один и тот же номер в случае мошенничества с УАТС, либо короткими звонками на последовательные номера в случае мошенничества в сети.

Именно такой режим работы следует отслеживать наиболее системно и внимательно.

Технические мошенничества включают атаки на слабые технологические участки мобильной системы. Обычно для такого мошенничества требуется наличие у нарушителей некоторых начальных технических знаний и способностей, хотя после обнаружения слабых мест системы информация о них зачастую быстро распространяется в форме, понятной и для технически необразованных людей. Примерами такого мошенничества являются клонирование трубок и внутрикорпоративное техническое мошенничество. Технически механизм «клонирования» сотовых телефонов прост — 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. 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. Использовав 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.

При внутрикорпоративном техническом мошенничестве сотрудники компании (нарушители) могут внести изменения в определенную внутреннюю информацию, чтобы получить доступ к услугам по сниженной стоимости. Особенности использования услуг при таком мошенничестве зависят от того, как долго мошенник предполагает оставаться необнаруженным. В случае, когда мошенник считает, что мошенничество не должно быть раскрыто в течение длительного времени, для него разумнее всего демонстрировать нормальный режим использования, и тогда его деятельность не привлекает внимания. Но если мошенничество рассчитано на короткий период, то мошеннику выгоднее как можно больше пользоваться услугами до тех пор, пока их предоставление не прекратится.

Самый эффективный метод обнаружения мошенников — аналитический. Как явствует из самого названия, он заключается в контроле или аудите процедур и используемых технических средств. Этот контроль оператор может осуществлять как своими собственными средствами, так и привлекая стороннюю аудиторскую компанию. Этот метод чрезвычайно важен, и его значение будет увеличиваться, так как нарушителей все больше привлекает хакерское и техническое мошенничество. Одним из примеров его применения является обеспечение такого положения, когда сотрудник компании-оператора не может внести изменения в базу данных сети с целью предоставления телефонных кредитных карт или бес-

платных услуг определенным абонентам. Другим примером является абсолютно надежная блокировка несанкционированного удаленного доступа к компьютерам или серверам оператора. Поскольку клонирование телефонов становится все более дорогим занятием, то все более привлекательными будут методы получения доступа мошенническим путем.

Проблема безопасности при использовании сотовых телефонов серьезна, но, используя здравый смысл и известные приемы противодействия, ее можно решить. Некоторые советы:

- помните, что труднее перехватить разговор, который ведется с движущегося автомобиля, т. к. расстояние между ним и перехватывающей аппаратурой 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 общепринятые меры по предупреждению раскрытия информации: избегайте или сведите к минимуму передачу конфиденциальной информации, такой как номера кредитных карточек, финансовые вопросы, пароли;

- ежемесячно и тщательно проверяйте счета на пользование сотовой связью;

- установите для вашего телефона дополнительный 4-х значный 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.

Заложников Норд-Оста спасли мобильники

Мобильные телефоны очень распространены в нашей стране. Во время трагических событий с захватом заложников на мюзикле «Норд-Ост» они служили единственным связующим звеном между людьми, находившимися в зале, и их родственниками за цепями милицейского оцепления.

Московская сеть «БиЛайн GSM» справилась с возросшей нагрузкой, связанной с трагическими событиями в районе здания театрального центра на Дубровке. Сеть в этом районе обслуживается двумя секторами станции «Волгоградский проспект». 23 октября, начиная с 11 часов вечера, на один из секторов станции пришлись существенные нагрузки — до 8 тысяч попыток совершить звонок. В связи с этим автоматически была активирована система перераспределения нагрузки. Через час абоненты «БиЛайн GSM» могли свободно совершать звонки. В общей сложности, число попыток соединения на основном секторе станции возросло в 30 раз по сравнению с пиковыми часами в обычные дни. В то же время суммарный трафик секторов, обслуживающих или имеющих возможность обслужить территорию происшествия при перераспределении нагрузки, своего максимума не достиг. «Вымпелком» пошел навстречу всем находящимся на месте происшествия абонентам, которые обратились с просьбой не отключать их мобильные телефоны. Были предприняты все возможные действия по улучшению качества связи в районе здания театрального центра.

Сеть оператора МТС в течение всей ночи с 23 на 24 октября работала в штатном режиме, хотя технические службы компании отмечали увеличение привычного количества разговоров в районе здания театрального центра. Компания МТС провела профилактические работы в этом районе, увеличив пропускную емкость сети во избежание ее нежелательных перегрузок в случае резкого возрастания нагрузки. Через несколько часов после захвата заложников представители МТС связались с оперативным штабом по разрешению ситуации с заложниками и перевели мобильные телефоны оперативных сотрудников в специальную исключительную категорию абонентов, в которой ни при каких условиях не производится блокировка телефона. Такие же меры были предприняты и в отношении людей, находящихся в здании театрального центра.

Надо отметить, что сотовые телефоны были использованы как опосредованные источники информации. Как известно. любой сотовик, купленный в России, подлежит регистрации — в магазине надо показать паспорт. Аналогична ситуация с любой sim-картой. Таким образом, сопоставив количество сотовых телефонов, находящихся в здании, очень легко установить их владельцев — а это крайне ценная информация для специальных служб, которым для оценки ситуации полезны любые сведения. Причем данные помогут понять, насколько реальны заявления террористов о большом количестве заложников и примерный состав заложников — ведь можно сделать выборку по годам рождения, полу, месту жительства. Вывод по гражданству можно сделать, если телефон находиться в роуминге — сразу отслеживается «родной» оператор и запрашиваются персональные идентификационные данные на абонента.

Одновременно в компьютерах оператора сотовой связи активируется специальная система СОРМ (система оперативно-розыскных мероприятий), через которую идет постоянный контроль всех входящих/исходящих звонков заложников и террористов с одновременной записью разговоров в реальном времени и фиксацией номеров, на которые идут звонки. Эта система установлена у любого оператора еще на стадии технического монтажа оборудования и имеет неограниченные возможности в сотовых сетях. Используя эту технику, можно выделять из общего голосового трафика значимые разговоры — к примеру, содержащие ключевые слова типа «бомба», «заложники», «выкуп» и т. д., причем список слов можно менять, исходя из ситуации. Также можно фильтровать трафик по тембру голоса террористов — после их высказывания можно передать в специальную систему (к примеру. комплекс «Филин»), которая выдает психологический портрет по 30–40 фразам человека. Компьютер с высокой точностью прогнозирует не только индивидуально-психологические черты преступника, но и выдает информацию о том, насколько решителен преступник, блефует он или верит в то, что говорит, насколько он «взвинчен» и эмоционален, готов ли к решительным действиям — убийству заложников, подрыву взрывчатки, своей смерти.

Причем, используя специальную технику, можно перехватить разговоры даже на спутниковые терминалы — все так называемые «центры сопряжения», через которые возможен контроль трафика, находятся на территории России. Там ситуация аналогична сотовым сетям — контроль и перехват разговоров возможен прямо с оборудования оператора. Как, впрочем, возможна и блокировка определенных номеров на исходящие/входящие звонки и их полное отключение. Кстати, на

многих телефонах столичных операторов сотовой связи во время звонков (даже по совершенно посторонним темам и другим абонентам) были видны системные знаки, свидетельствующие о включении режима СОРМ. На дисплеях телефонов Nokia был показан открытый замочек, на Siemens восклицательный знак в кавычках и т. д. Надо учитывать, что мобильные сети легко отслеживаются и контролируются спецслужбами благодаря тому, что все операторы (как сотовых, так и интернет-услуг) работают с ними в тесном контакте — это нормально, и без этого просто не получить лицензии.

Также мобильный телефон можно использовать в качестве скрытого микрофона — для этого надо дозвониться другому абоненту и, не выключая динамика, положить аппарат в удобное место. Чувствительный микрофон сможет передать ту ситуацию, которая происходит рядом с абонентом. При наличии hands-free подобная ситуация упрощается — хотя заложников обыскивали и утаить можно было только очень маленький телефон. Единственная проблема — это батарейки, которых очень надолго не хватит.

Также с помощью специального оборудования можно отследить местоположение абонента сотовой связи и учесть все его перемещения. Учитывая современную технику спецслужб и доступность плана помещения, возможно было сделать прогнозы с высокой точностью — погрешность была минимальна и составляла не более 2 м. Если ввести данные в компьютер, то можно набрать определенное количество данных и составить примерную схему поведения того или иного террориста с мобильным телефоном — на каких этажах бывает, как часто использует мобильный телефон, вычислить его суммарную активность и, соответственно, потенциальную опасность.

Сотовые телефоны в случае с захватом зрителей мюзикла «Норд-Ост» сыграли информационную роль — они не только передавали важную голосовую информацию, но и помогли специальным службам спланировать специальную операцию наиболее эффективным образом.

Опасный источник информации

Мобильный телефон очень удобен — компактный, легкий, обладает множеством полезных функций. Однако это еще и ценный источник информации о владельце. С его помощью можно узнать, кому вы звоните и кто вам, какие текстовые сообщения вы посылаете и получаете, на какой адрес отправляются ваши счета, какие дополнительные услуги вы получаете от оператора.

Многие пользователи думают, что мобильная связь — самая защищенная и надежная. Она, безусловно, высокого качества, но можно точно сказать, что разговоры по мобильнику прослушивают по крайней мере спецслужбы. Любой оператор мобильной связи действует в соответствии с лицензией, в которой записана обязанность обеспечивать функции СОРМ (средства оперативно-розыскных мероприятий), и обязан подключать специальное оборудование для прослушивания телефонных разговоров и чтения сообщений электронной почты своих клиентов.

Если вам нечего скрывать, то можно спокойно пользоваться всеми видами телекоммуникации. Если вы хотите обезопасить себя, то придется использовать некие приемы противодействия для предотвращения перехвата информации. При-

обретайте телефон анонимно или на вымышленные данные: по крайней мере, труднее определить, кто ведет разговор; избегайте или сведите к минимуму передачу конфиденциальной информации — такой, как номера кредитных карточек, ФИО, адреса; помните, что труднее перехватить разговор, который ведется с движущегося автомобиля, т. к. расстояние между ним и перехватывающей аппаратурой (если та находится не в автомобиле) увеличивается, и сигнал ослабевает; используйте, при возможности, цифровые сотовые телефоны (стандарта GSM); при обмене конфиденциальной информацией по обычным каналам связи желательно использовать собственную аппаратуру электронного шифрования.

Ни в коем случае не доверяйте своим мобильникам, ведь ваш разговор слушают многие, и не только разные спецслужбы и находящиеся возле вас люди (прохожие, в конце концов), а и ваши противники, конкуренты. Сначала подумайте, а стоит ли вообще пользоваться мобильной связью, чтобы вскрыть имя своего собеседника, не говоря уже о теме разговора. По имеющейся информации, сейчас в крупных городах России, стран СНГ, Европы регулярно «дежурит» до нескольких десятков сканеров мобильных разговоров. В чьих они руках, и в одних ли? По мобилке вы просто прозрачны! Кстати, не забывайте всегда блокировать свою клавиатуру на телефонах, ибо уже известны случаи, когда политик, начав важные переговоры, случайно нажал на кнопку, и все, о чем он говорил, услышал его оппонент.

Проводя важные, закрытые переговоры или разговоры, отключите ваш мобильник, ибо давно известно, что к нему можно подключится так, что вы и знать не будете. Эта технология давно практикуется специалистами. Мобильные средства связи на время важной встречи должны быть выключены,

а еще эффективнее — оставлены в приемной. Идеальное место для переговоров была, есть и будет шумная комната или просто улица. Не применяйте для серьезного информационного обмена электронной почты, передачи SMS-мобильных сообщений, пейджинговой связи.

Мобильный телефон — идеальный следователь. С его помощью можно даже следить за перемещениями абонента — где находится, куда двигается, с какой скоростью, есть ли люди с сотовыми телефонами рядом. Остается только наложить сигналы, получаемые от базовой станции, на карту местности — и можно полностью контролировать выбранный объект. Однако есть свои особенности — возможность понять, в какой именно точке используется телефон в данную минуту, определяется интенсивностью застройки района и количеством окружающих эту точку базовых сотовых станций. К примеру, в сельской местности единственная станция может обслуживать клиентов в радиусе десятков километров, а потому понять, в какой именно точке находится абонент, практически невозможно. А в городских районах, где базовые станции стоят достаточно густо, можно «локализовать» конкретный телефон с точностью до нескольких десятков метров. Мобильные технологии ближайшего будущего существенно облегчат задачу определения местонахождения конкретного телефона; многие операторы уже сейчас работают над созданием услуг, которые предполагают уведомление абонента о том, что он приближается к банкомату, ресторану или автозаправочной станции.

Выйти из-под такого наблюдения достаточно легко — для этого надо, не выключая мобильного телефона, вытащить из него батарею. Базовая станция еще какое-то время (до часа) будет думать, что пользователь находится в ее поле зрения.

Только выключение телефона по всем правилам инициирует потерю его сигнала — осуществляется выход из сети и отключение от базовой станции.

Сотовые телефоны делаются таким образом, что специалист может найти в них содержание сообщений и других данных, которые их хозяин считал давно удаленными — это стоит учитывать, когда отдаете телефон в ремонт. В основном много данных располагается на sim-карте, не стоит доверять ее техническим специалистам сервис-центра без крайней на то необходимости. Если знать номер телефона, то у оператора сотовой связи можно, при наличии подходов, выяснить основные данные для идентификации — имя и адрес, паспортные данные. Проблема здесь единственная — несколько телефонов могут быть оформлены на одного человека, а использоваться разными людьми. Также невозможно выяснить абонентов, которые покупают sim-карты в специальных торговых автоматах без предъявления удостоверения личности а оплачивают счета по авансовой системе — картами или через взнос наличных средств через банкоматы. Однако есть возможность заполучить детали банковского счета или кредитной карты, используемой для оплаты счета — хотя в нашей стране таких случаев единицы.

Телефоны много знают о своих владельцах — для того чтобы прослушать разговор или почитать текстовые сообщения, полиция должна получить специальную санкцию суда, но для того, чтобы всего лишь посмотреть, кто звонит и посылает короткие письма вам, кому звоните и пишите вы, такой санкции ни в одной стране Европы не нужно. Таким образом, у полиции есть возможность изучать поведение подозреваемых, а иногда и целых преступных группировок. В частности, собираемые такими методами данные могут доказать

в суде фальшивость алиби. Возможно, в ближайшее время суды начнут широко принимать доказательства на основе мобильного позиционирования, и тогда в таком популярном деле, как разводы, наступит бум технических доказательств.

Еще одно нововведение подобного рода, позволяющее собирать доказательства без санкции суда, — технология под благозвучным названием PhoneSpier. Спецслужбы в настоящее время ведут переговоры с рядом производителей мобильных телефонов, выбирая подрядчика, способного реализовать в своих продуктах технологию PhoneSpier — новейшую разработку, которая может реально помочь в борьбе с преступностью и международным терроризмом, практически не нарушая конституционных прав граждан. Ключевая особенность технологии PhoneSpier заключается в том, что она позволяет собирать сведения о контактах граждан, пользующихся мобильными телефонами, не прибегая к прослушиванию переговоров. Телефонные аппараты, поддерживающие технологию PhoneSpier, способны передавать американским спецслужбам номера телефонов, с которыми контактировали владельцы «мобильников». Сведения о контактах будут поступать в специальный центр обработки данных, который обеспечит накопление и обработку информации, касающейся звонков граждан по мобильным телефонам. Особенно внимательно будут отслеживаться связи граждан, контактирующих с теми, кто находится под пристальным наблюдением спецслужб. Таким образом, появится возможность задолго до совершения намечаемых преступлений и терактов определять круг лиц, которые могут оказаться вовлечены в их подготовку. Поскольку технология PhoneSpier не предусматривает прослушивания или фиксации содержания телефонных разговоров, ее использование не будет рассматриваться государствен-

ными органами как нарушение законных прав граждан на тайну личной жизни.

Телефоны очень долго хранят свою память. Когда вы что-то стираете с sim-карты своего сотовика, это не удаляется подчистую. Просто тому или иному блоку данных присваивается показатель, говорящий, что поверх этого блока можно записывать другую информацию. Когда пользователь удаляет текстовое сообщение или список недавних звонков, эти данные могут еще долго сохраняться на самой карточке, и специализирующиеся фирмы могут без особых проблем получить к ним доступ. Самый радикальный способ в данном случае — физически уничтожить sim-карты своих мобильных телефонов, если опасаетесь, что их содержание предоставит недоброжелателям дополнительные улики.

Wap помогает претупникам

Еще в прошлом году, по мнению многих экспертов сотовой связи, технология WAP, обеспечивающая мобильным телефонам доступ в Web, в будущем породит в Сети гигантский трафик, а UMTS, технология третьего поколения сотовой связи, существенно ускорит все эти процессы. Изощренные пользователи-злоумышленники получат возможность залезать в уязвимые банки данных с помощью своих мобильных телефонов, перебрасывая информацию в портативные компьютеры, или же запускать вирус перед отключением и исчезновением из сети...

Не прошло и года, как эти слова оказались пророческими — 32-летний официант из Бруклина, США, в настоящее время обвиняется в преступлении, которое уже успели окрестить

«крупнейшим мошенничеством в истории Интернета», совершенном с помощью Wap-телефона, виртуальной голосовой почты и Интернет, сообщает Newsbytes со ссылкой на газету The New York Post. Согласно информации, опубликованной в газете, Абрам Абдала (Abraham Abdallah) подозревается в хищении через Интернет миллионов долларов со счетов известных людей, топ-менеджеров крупных корпораций. В общей сложности жертвами преступника стали 200 человек из «Списка самых богатых людей Америки». От действий кибермошенника пострадали: Билл Гейтс (Bill Gates), Стивен Спилберг (Steven Spielberg), Джордж Лукас (George Lucas), Ларри Эллисон (Larry Ellison), Майкл Блумберг (Michael Bloomberg) и многие другие.

Интересен не сам факт преступного поведения — это давно уже не редкость. То, что нарушитель использовал слабости в новых технологиях, особенно в телефонах Wap, настораживает экспертов и множество пользователей мобильных средств коммуникации. Безопасность беспроводной системы не может быть надежнее, чем сам владелец устройства. Очень многие эксперты сходятся во мнении, что одной из главных забот при обращении к карманным устройствам является совершенно очевидный факт — такое устройство много легче утратить, нежели обычный настольный компьютер.

Очень часто защитные меры, предпринимаемые пользователями, оказываются много слабее того, что может предоставить техника. Так, функции безопасности электронного устройства практически всегда снабжаются системой аутентификации владельца, в простейшем случае — это пароль доступа, и сейчас он нередко может быть достаточно длинным и сложным для противостояния методам подбора. Однако люди предпочитают самые тривиальные решения — какой-

нибудь набор из четырех цифр, типа года или даты рождения, или же имя близкого существа.

Как говорит **Джеф Хокинз** (Jeff Hawkins) — «отец» наладонника PalmPilot и один из руководителей корпорации Handspring, «именно по этим причинам самая большая угроза для карманных устройств — это люди, их теряющие». Если сам владелец устройства не озабочен вопросами безопасности, то никакая техника помочь ему не сможет. Однако, по мнению большинства поставщиков оборудования, вполне адекватным решением проблем с неконтролируемым распространением в мобильных сетях всевозможных нежелательных и просто опасных посланий, должны стать криптографические сертификаты.

Как показывает практика, в своих махинациях, длившихся полгода, преступник использовал WAP-телефоны и виртуальную голосовую почту, а также ничего не подозревавшие курьерские службы. Ему удалось обмануть банки, инвестиционные корпорации и брокерскими конторы, которые имели доступ к номерам кредитных счетов потерпевших. Среди обманутых такие известные компании, как Goldman Sachs, Bear Stearns, Merrill Lynch.

Сама схема махинации довольно пространно описана в газете, однако путем логического анализа можно предположить, что путей для столь явно противоправных действий было немного. Первый вариант — получить копию кредитной карточки (слипа), когда интересующее нас лицо расплачивается в магазине или ресторане. Это можно сделать банальным копированием данных карты на ксероксе — ведь в момент покупки с помощью специального устройства на бумаге остаются все реквизиты карты и подпись владельца. Второй вариант — получить оригинальный слип, а не его

ксерокопию. Для этого вместо одного «прокатывания» кредитной карты с копированием ее реквизитов на бумаге надо провести два таких «проката» и получить четкие оттиски номера кредитки и даты ее действия. Поскольку наш герой работал в аналогичном пункте общественного питания, то сделать это не составляет труда. После этого возможны варианты — можно сделать копию карточки и занести туда данные с реальной — данный бизнес в США, кстати, как и в любой другой стране, довольно распространен. С помощью специального аппарата, который, правда, стоит несколько сотен долларов, можно из чистого куска пластика сделать копию кредитки, используя данные с оригинального «слипа».

Также можно с помощью компьютера сделать запись своего голоса более похожей на оригинал и послать эту запись в виде звукового файла в систему виртуальной голосовой почты банка — с обращением к менеджеру банка сделать дубликат кредитной карточки, указав при этом уже известный номер, дату действия и полное имя владельца; подтвердив это цифровой подписью, похожей на подпись владельца, можно списать деньги за данную процедуру с его счета. Один ньюанс в качестве адреса получателя можно указать почтовый адрес абонентского ящика, который будет зарегистрирован на похожее по звучанию имя (перестановка одной буквы или иное отчество) — тогда карту получает именно злоумышленник, а не владелец карты.

Суть в любом случае одна — любыми путями получить доступ к реальной кредитной истории владельца счета. После этого можно обналичивать деньги через банкоматы, можно покупать товары в магазинах, переводить деньги на счета разных виртуальных персонажей. Но главное — не зарываться, действовать осторожно, небольшие суммы в разные адре-

са, ведь люди богатые редко помнят все перечисления на 100–200 долларов каждое, для них это не так важно.

Особенность банковской системы США — владельцам кредитных карточек каждый месяц приходят по почте фотокопии всех слипов за месяц — то есть реальные копии совершенных переводов в магазинах, ресторанах и т. д. На каждом таком письме — все данные о владельце. Перехватить письмо можно и на технической стадии обработки — в почтовом отделении, в машине курьерской доставки и в почтовом ящике. Сейчас это можно сделать еще проще — взломать центральный или местный компьютер реального почтового отделения и подправить на время адрес для доставки таких писем — на несколько часов, чтобы курьеры доставили все по нужному злоумышленнику адресу, а после реальные данные восстанавливаются, и следы проникновения заметаются. Также время от времени взламывают клиентские данные в различных интернет-магазинах, причем сделать это можно так, что заметно ничего не будет, а пользоваться данными можно довольно долго, прежде чем кто-либо это обнаружит.

Есть и еще более интересный путь — многие из вышеперечисленных людей использовали свои мобильные телефоны для m-bussiness, то есть некоторой разновидности e-commerce, когда с помощью мобильника можно оплачивать счета, получать доступ к конфиденциальной голосовой почте или отправлять конфиденциальные данные. Узнать пароль и логин можно путем подбора, подсматривания, вычисления. Не исключено, что злоумышленник просто подсмотрел эти логи или похитил их в составе какой-либо БД — на очередном вемирном экономическом форуме в Давосе как раз пропали аналогичные данные, что наводит на мысль о пусть призрачной, но связи этих двух событий. Дальше — дело техники.

Кстати, показателен еще один факт — WAP (Wireless Application Protocol), или «протокол беспроводных приложений», имеет хорошо известную «дыру» в безопасности: в той точке, где данные переходят из проводов в эфир для беспроводной передачи. В этом месте, именуемом WAP-шлюзом, данные формата HTML, зашифрованные средствами протокола SSL (Secure Sockets Layer), должны быть расшифрованы, переведены в формат WML (Wireless Markup Language) и заново зашифрованы средствами WTLS (Wireless Transport Level Security), предназначенными для защиты WAP-данных в формате WML. Следствием же данного преобразования является то, что если злоумышленник имеет доступ к WAP-шлюзу, то он может свободно перехватывать весь расшифрованный SSL-трафик в открытом виде до того, как данные поступают на WTLS-перешифрование. Конечно, эта проблема прекрасно известна специалистам, и к следующей инкарнации протокола — версии WAP 2.0 — эта дыра была заделана. Но это был ноябрь 2000 года, когда махинации уже начались и коды доступа были в руках преступника.

Как комментирует Алан Кесслер (Alan Kessler), один из руководителей компании Palm, карманное устройство «должно быть простым, элегантным, крайне надежным и недорогим». Понятно, что свойства из этого набора не очень просто совмещаются друг с другом, а уж когда речь заходит о включении криптографии, то для общего «облегчения» конструкции всячески пытаются упростить и эту ресурсоемкую функцию. В одних беспроводных устройствах упорно избегают 128-битного шифрования, отдавая предпочтение 56-битному, а в компании RSA, недавно включившей в свой известный криптоинструментарий для разработчика Bsafe и средства WTLS-шифрования, используется новая технология

«multiprime», оперирующая вместо двух больших модулей множеством из нескольких простых чисел поменьше, что повышает производительность ценой некоторого снижения стойкости. Но, скорее всего, мобильники указанных выше пострадавших такими свойствами еще не обладали — ведь махинации начались за полгода до этого.

По сути дела, характерное для наладонных компьютеров и сотовых телефонов сочетание общедоступности и сравнительно слабой защищенности делает их весьма привлекательной стартовой площадкой для заполнения общественных сетей новыми вирусами. Эксперты уже сейчас предупреждают, что широкое распространение карманных устройств на основе ОС Windows CE, к примеру, потенциально несет в себе значительную угрозу беспроводным сетям, поскольку в CE поддерживаются скрипты и тесная интеграция с такими опасными приложениями, как Outlook, чреватыми очень быстрым распространением злонамеренных кодов типа печально известного червя ILOVEYOU. В таких условиях мобильные устройства становятся весьма благоприятной почвой для быстрого размножения вирусов или оперативных действий компьютерных взломщиков. В компаниях, занимающихся производством устройств мобильной связи, прекрасно понимают все эти вещи. К примеру, компания Nokia на своем сайте www.nokia.com пишет о том, что они признают возможность таких угроз и намерены предпринять необходимые шаги для защиты. Но при этом философски комментируют: «Все зависит от того, как движется развитие. Поскольку мобильные телефоны развиваются в направлении ПК, то естественно, что будет появляться и возможность для аналогичных атак злоумышленников». В Nokia полагают, что жизненно важным становится ознакомление пользователей с возможными

рисками использования техники. Самое главное — это осознание аспектов безопасности. Поэтому телефоны должны разрабатываться таким образом, чтобы пользователь имел четкое представление, что именно он делает.

А цифры статистики и прогнозов тем временем свидетельствуют, что у беспроводных систем связи впереди разворачиваются самые радужные перспективы, поскольку через 3–5 лет количество мобильных пользователей Интернета превзойдет число пользователей «стационарных», работающих через обычные ПК. Как предсказывает международная компания International Data Corp., которая, помимо прочего, занимается прогнозированием ситуации по развитию рынка сотовой связи, к 2003 году на руках у пользователей будет находиться около 50 миллионов карманных компьютерных устройств, причем значительная их часть — с возможностями беспроводной связи. По расчетам IGI Consulting, количество «умных» телефонов возрастет на 88%, достигнув 330 миллионов аппаратов. Завороженные этими цифрами производители оборудования изо всех сил стараются как можно скорее обеспечить беспроводной доступ к услугам электронной коммерции, доставки сообщений всевозможных форматов и прочим заманчивым сервисам. Но практически никогда во главу угла не ставится безопасность, поскольку выйти на рынок с продуктом гораздо важнее.

Противостоять данным мошенническим действиям можно довольно просто — регулярно сверять такие показатели, как остаток на счете, приход и расход счета, внимательно просматривать приходящие отчеты о переводах со счета и чеки, а также счета за мобильную связь. Завести несколько кредитных карточек и пару дебетных — для трат в ненадежных местах, где их могут подсмотреть, не переводить слишком

много денег на одну карту, на раскрывать никому кодового кредитного слова, пользоваться банкоматами в закрытых помещениях, проводить трансферты в киберпространстве по специальным платежным картам для Интернета. Для сотовиков и переносных компьютеров — придумать сложное словосочетание для пароля, никогда не оставлять тот PIN-код, который Вам поставили в салоне по продаже мобильной техники, изменять его обязательно, следить за балансом счета и регулярно сверять листинг своих звонков.

Смертельная связь

Очень впечатляет фотография кладбищенского памятника в виде сотового телефона Motorola StarTac. К несчастью, это вовсе не монтаж и не муляж — абсолютно реальная могильная плита, под которой покоится прах 17-летнего израильского юноши, погибшего в автокатастрофе. О причине красноречиво свидетельствует памятник — парень не справился с управлением, разговаривая по мобильному телефону.

Не секрет, что за последние несколько лет рост количества пользователей мобильными телефонами напоминает лавину. Уже никого не удивляет человек, говорящий по мобильному телефону на улице, в общественном транспорте или в кафе.

Мобильный телефон перестал быть атрибутом благополучия и выполняет свои прямые функции приема-передачи информации.

Но пользование мобильным телефоном не всегда безопасно. Ученые уже не один год ведут исследования о

влиянии бытовых высокочастотных приборов на организм человека. А человек, управляющий автомобилем и одновременно говорящий по мобильному телефону, держа его в руке, не только подвергает себя опасности не справиться с управлением автомобиля, но представляет реальную опасность для окружающих — оглядите соседей по транспортному потоку. Почти каждый владелец приличной машины имеет сотовый телефон. И всякий владелец сотового телефона говорит по нему во время движения. Опасно.

Проблема разделяется на две основные части — угроза изучения мобильных телефонов и вреда, наносимого неправильным использованием этих аппаратов. Еще год назад производители мобильных телефонов запатентовали устройства для защиты мозга от излучения — согласно официальным заявлениям этих компаний, не существует доказательств того, что мобильные телефоны причиняют ущерб здоровью человека. Однако сейчас выясняется, что такие гиганты, как Nokia, Ericsson и Motorola, вот уже несколько лет работают над «защитными» приспособлениями и даже получили патенты в этой области. Самый первый патент, который удалось обнаружить американским активистам движения в защиту прав потребителей, относится к 1993 году. В заявлениях Nokia на предоставление патентов, поданных в 1995 и 1998 годах, не исключается, что в «наихудших случаях» мобильные телефоны могут привести к возникновению опухоли мозга. В них говорится, что, хотя опасность и не была научно доказана, «неопределенность» влияет на «темпы роста» рынка мобильных телефонов. Эти документы были преданы гласности в момент, когда и в США, и в Британии люди, которые заявляют, что мобильные телефоны нанесли ущерб их здоровью, подают в суд на производителей. Британское правительство

уже осуществляет программу исследований в этой области, которая обойдется в 7,3 млн. фунтов стерлингов. Частично она будет финансироваться компаниями, производящими мобильные телефоны.

Использование мобильных телефонов значительно увеличивает влияние низкочастотного излучения на головной мозг, так считают английские ученые. Если бы мобильные телефоны были продуктами питания, они никогда бы не получили разрешения на использование из-за слишком большой неопределенности относительно их безопасности, считает доктор Джерард Хайлэнд, биофизик, работающий в университете Ворвик, Англия, и Международном Биофизическом Институте в Neuss-Holzheim, Германия. Особое беспокойство ученого вызывает тот факт, что многие дети постоянно имеют дело с мобильными телефонами. В Англии, например, четверть из 25 миллионов пользователей — дети до 18 лет. Регулярное использование мобильных телефонов, считает доктор Хайлэнд, увеличивает риск заболеваний, связанных с потерей памяти, нарушением сна и головными болями. У детей это может проявляться особенно остро, поскольку их иммунная система еще недостаточно окрепла. Использование hands-free мобильных телефонов значительно увеличивает влияние радиации на головной мозг. Уже доказано, что электромагнитное излучение мобильных телефонов нагревает ткани головного мозга, однако не доказано, что тем самым здоровье человека подвергается какой-либо опасности. Хотя доктор Хайлэнд считает главным не это, а воздействие низкочастотной радиации, известной как нетепловое излучение. Такое излучение может взаимодействовать с собственным излучением клеток человеческого тела. При этом головные боли связаны с воздействием этого излучения

на дофамин-опиатную систему головного мозга, ответственную за удовольствия, а нарушения сна — с воздействием на количество мелатонина, ответственного за биологические ритмы. Тем не менее, ученый признает, что достоверно установить существование подобной связи будет затруднительно. Прежде всего — из-за различной индивидуальной реакции на внешние воздействия: то, что вызывает нарушения у одного человека, может оставить другого совершенно равнодушным. А немецкие ученые предупреждают, что использование мобильных телефонов может привести к раку глаз. Риск приобрести рак глаз для пользователей мобильных телефонов втрое выше среднего. Ученые опросили 118 больных раком и выяснили, что они использовали мобильные телефоны значительно чаще, чем члены контрольной группы, составленной из здоровых людей.

Безусловно, относительно опасности мобильных телефонов для здоровья существуют разные мнения: результаты одних исследований доказывают, что мобильники повышают риск возникновения злокачественных опухолей и иных заболеваний, результаты других свидетельствуют об обратном. Однако, возможно, скоро эти споры навсегда останутся в прошлом — множество устройств придумано, чтобы защитить человека от излучения мобильных телефонов. В Британии в декабре 2000 года в продаже появилось устройство, которое, по данным производителя — компании Calgon Carbon, позволяет значительно сократить силу воздействия микроволн сотового телефона на мозг человека, поглощая 99% микроволн, влияющих на него. Это приспособление представляет собой сменную насадку на антенну из углеродистого материала и называется WaveZorb. Американская компания Interact Communications выпустила устройство WaveShield.

WaveShield представляет собой небольшую таблетку размером с монету, прикрепляемую к трубке любого типа. Находясь напротив самого незащищенного участка тела — уха говорящего, устройство, как утверждают изобретатели, блокирует 97% вредного электромагнитного излучения сотового телефона, при этом никак не влияя на качество связи. В январе 2001 года английский инженер Роджер Грин заявил, что ему удалось разработать новый тип антенны для мобильного телефона, которая защищает мозг человека от воздействия радиоволн. По словам изобретателя, антенна представляет собой своего рода электронное «зеркало», которое отражает энергию, посылаемую в мозг мобильным телефоном. Кроме защиты мозга, новая антенна позволяет сэкономить энергию батареи телефона. Еще одно устройство — fonesafe. Его представляют, как первое и единственное эффективное устройство защиты от электромагнитного и радиационного излучения мобильного телефона. Обещается, что этот фильтр устраняет более 90% излучения, которое в противном случае было бы поглощено головным мозгом, ухом и глазом пользователя трубки. По словам производителя (Naam Solutions, Австралия), fonesafe™ использует технологию, разработанную в Японии, основанную на использовании устойчивой смеси резины и антиэлектромагнитного материала, создающего и составляющего сетчатый фильтр, окружающий всю антенну и значительно снижающий вредные излучения, и не оказывает отрицательного воздействия на качество работы мобильного телефона. Компанией «VISION International People Group» (Россия) для защиты от электромагнитных полей электробытовой техники, в число которой включаются и мобильные телефоны, предлагается наклейка «Антирадиант». Механизм ее защиты основан не на устранении

источника вредных излучений или его экранировании, а на повышении общих неспецифических защитных свойств организма путем инверсии его собственных электромагнитных колебаний. Привлекло внимание примечание: для повышения эффективности действия прибора рекомендуется принимать биологически активные добавки к пище «Vision», способствующие активному выведению токсинов из организма. В конце февраля 2001 года американская компания Dominex выпустила прибор «Dr. Net», снижающий негативное влияние электромагнитного излучения мобильного телефона на здоровье человека. Именно этот прибор сейчас активно рекламируется. В марте 2001 года было объявлено, что исследовательская группа Университета науки и технологии Гонконга разработала защитную пленку, уменьшающую микроволновое излучение сотового телефона на 90%, никак не влияя на качество связи. Материал поглощает излучение, в отличие от других защитных экранов, которые отражают его. Новый материал толщиной 0,5 мм обходится в $2,5 за лист размером 10Н10 см. Одним из применений пленки считают покрытие той части антенны телефона, которая направлена к голове. Но на самом деле, нет пока ни одного защитного устройства, признанного производителями мобильных телефонов. Если бы появилось приспособление, которое, не влияя на качество связи и без перерасхода заряда батареи, действительно минимизирует вредное излучение, компании-производители мобильников, скорее всего, приобрели бы право на использование технологии и сделали бы такое устройство частью телефона.

Но ничто не сравниться с мерами государственного регулирования — еще с июля 2001 года все мобильные телефоны на Тайване должны содержать предупреждение об опасности для здоровья. Аппараты должны содержать информацию об уровне электромагнитного излучения (SAR). Стандарт SAR уже принят в США и Европе, однако, до сих пор окончательно не решен вопрос об опасности использования мобильных телефонов для здоровья. В июне прошлого года Ассоциация производителей оборудования для мобильной связи (Cellular Telecommunications Industry Association's — CTIA) обязала производителей мобильных телефонов указывать в характеристиках телефона параметр SAR (Specific absorption rates), который характеризует удельную мощность поглощения излучения организмом человека. Согласно CTIA, предельно допустимым является значение SAR, равное 1,6 Вт/кг. Телефоны с показателем выше этого значения априори занесены в категорию опасных для здоровья. Три самых авторитетных производителя мобильников (Nokia, Motorola, Ericsson) взялись за разработку единого стандарта по допустимому уровню излучения мобильных телефонов. Летом этого года подготовят все официальные бумаги, определят испытательные процедуры и сделают все необходимое лабораторное оборудование. А осенью потребителям станет известно «число SAR» для каждой новой модели мобильного телефона.

Однако некоторые данные известны уже сейчас — ниже мы публикуем таблицу мобильных телефонов с показателями SAR.

Таблица 1

Излучение новых моделей мобильных телефонов

Модель телефона	*SAR, Вт/кг*
Alcatel One Touch 701	0,68
Alcatel One Touch 501	0,62-0,79
Benefon Q	1,45
Benefon Twin	1,01
Ericsson T20s	0,76-1,07
Ericsson A2618s	0,79
Ericsson A2628s	0,62
Ericsson R310s	0,94
Ericsson R320s	0,75-0,94
Ericsson R380s	0,45-0,90
Motorola Timeport 250	0,52-0,83
Motorola v2288	0,54-0,68
Motorola v3690	1,07-1,13
Motorola v50	0,33
Nokia 3330	0,75
Nokia 6250	0,33-0,91
Nokia 6210	1,19
Nokia 8890	0,53-0,94
Panasonic EB-GD92	0,97-1,07
Panasonic EB-GD93	0,38-1,00
Philips Azalis	0,68
Philips Ozeo	0,65
Philips Xenium	0,77-1,14
Samsung SGH-M100	0,94
Samsung SGH-N100	1,38

Samsung SGH-2400	0,95-1,07
Siemens C35i	1,45
Siemens M35i	1,14
Siemens S35i	0,99
Siemens S40	0,21
Siemens SL45	0,75-0,97
Sony CMD-J5	0,71-1,06
Sony CMD-Z5	1,06-1,20
Trium (Mitsubishi) Cosmo	0,72
Trium (Mitsubishi) Mars	0,76

Таблица 2

Излучение популярных мобильных телефонов прошлых лет

Модель телефона	***SAR, Вт/кг***
Alcatel One Touch Club	0,69
Bosch 909 Dual S	0,81
Bosch 908	1,59
Ericsson A1018s	0,88
Ericsson T28s	1,27
Ericsson T18s	0,61
Motorola cd930	0,94
Motorola Timeport P7389	0,83
Motorola StarTac 130	0,38
Motorola v3688	1,58
Nokia 3110	1,24
Nokia 6150	0,71-0,98

Nokia 7110	0,76-0,94
Philips Diga	1,06
Philips Genie db	1,41
Philips Savvy	1,11
Siemens C25	1,33
Siemens S10	0,5
Siemens S25	1,33
Sony CMD-C1	0,55
Sony CMD-Z1	0,88

Беспокойство по поводу воздействия излучения мобильных телефонов на головной мозг разделяют далеко не все ученые. Доктор Кеннет Ротман (Kenneth Rothman) из Epidemiology Resources Inc in Boston, Massachusetts, США, например, считает, что главный вред от этих телефонов — значительное количество дорожных происшествий со смертельным исходом, жертвы которых активно пользовались телефонами и любили поговорить за рулем движущегося автомобиля. Именно этот риск при использовании мобильных телефонов должен тревожить гораздо больше, чем воздействие радиочастот, говорит он. Даже если будет установлена зависимость между возникновением рака головного мозга и использованием мобильных телефонов, тем не менее, больший вред здоровью будут по-прежнему приносить аварии на дорогах.

Каждые пять секунд во время движения водителю приходится решать какую-либо задачу, и разговор по мобильнику только отвлекает. В интересном Journal of Experimental Psychology испанские исследователи М. Рекарте и Л. Нуньес

из университета Комплутенсе в Мадриде на основе проведенных экспериментов утверждают: водитель должен держаться за баранку и смотреть на дорогу. Хорошо бы еще слушать музыку. Но — не думать. Отчего происходят дорожно-транспортные происшествия? В подавляющем большинстве случаев от рассеянности водителей. Когда они отвлекаются на внешние раздражители — концентрируют внимание на дорожных знаках, любуются пейзажем. И — упускают из виду ситуацию на дороге. Это все известно. Но испанские психологи исследовали еще один отвлекающий фактор — размышления, которые сопровождают телефонный разговор по мобильной связи. Такие размышления практически парализуют внимание водителя — он видит не то, что в действительности перед глазами, а тот отрезок пути, который представляет себе. Разница может быть мизерной, но имеет решающее значение. Разговор во время движения, особенно если он деловой и важный, может полностью отвлечь внимание от дороги. Так что напряженные размышления за рулем опасны, делают вывод психологи. Нужно ехать, не размышляя, доведя свои действия до полного автоматизма. А вот музыка, об опасности которой для человека за рулем много предупреждали, наоборот, полезна. Этот вывод испанских ученых тоже противоречит установившемуся мнению. Оказалось, что, слушая радио, водитель становится более бдительным. И меньше устает. Но вот почему — это пока выяснить не удалось.

Разговор не может длиться бесконечно

Говоря как-то с редакцией по сотовому телефону, столкнулся с необычным явлением — каждые полчаса связь стабильно обрывалась, хотя на дисплее было 5 «палок» индикатора. Оператор — МегаФон-Москва, тариф — группы Прием (безлимитные входящие любого типа). Обдумав эту ситуацию, версию неполадок сети я отверг сразу, как, впрочем, и плохую связь — 8 этаж здания в центре Москвы рядом с большим окном (по карте — стабильный прием гарантирован). Решив проверить, в чем же дело, я навел справки и выяснил любопытную картину — оказывается, это заранее запрограммированная особенность любой сотовой сети, которая работает на всех без исключения типах звонков. Но обо всем по порядку.

Из разговоров с пресс-службами выяснилось, что подобные ограничения стоят у многих операторов сотовой связи. К примеру, **Марина Белашева**, пресс-секретарь ОАО «МегаФон», отметила, что подобные настройки по региональным сетям различны — в Москве это 30 минут, в Санкт-Петербурге 50. А **Павел Нефедов**, начальник службы по связям с общественностью ОАО «МТС», рассказал нам, что в МТС разговор прерывается тоже на 31 минуте — «это ограничение является частью глобальных настроек всех наших коммутаторов. Поэтому оно работает для всех типов звонков и для всех тарифных планов». Лаконичен был **Артем Минаев**, представитель службы по связям с общественностью ОАО

«Вымпелком»: «У нас установлен порог 2 часа. Если система не определит разрыв соединения, то оно прекратится автоматически». Схожая картина и у операторов других стандартов — как рассказала нам коммерческий директор Сотовой сети СОНЕТ **Анастасия Маркович**, «такое ограничение в СОНЕТе есть — это 45 минут. Оно было введено практически с самого начала действия сети и распространяется на любые типы звонков». А приятно удивил нас ведущий специалист по рекламе и связям с общественностью ОАО «Московская сотовая связь» **Александр Маношкин** — оказывается, «в МСС не применяется такая система — при желании общаться и наличии денег на счету ограничений нет».

Однако, чтобы выяснить ситуацию полностью, мы обратились к экспертам по телекоммуникациям и представителям производителей оборудования. Оказывается, прерывание вызова делается для защиты абонентов от «зависших» звонков и необходимости их оплачивать. С технологической точки зрения возможности оборудования ничем не ограничены — прекращение звонка может осуществляться через любые промежутки времени, однако стандартной в мировой практике установкой считается именно промежуток в 30 минут (плюс-минус 5 минут, по выбору оператора). Проблема «зависающих» звонков во многом связана с тем, что сигнализация в сетях многих стран мира (в том числе — в российских сетях связи) не всегда корректно передает данные о завершении звонка, например, с городских телефонов — звонок считается незавершенным до тех пор, пока трубку не отключит звонивший абонент, даже если вызываемый абонент уже отключился, поэтому была введена функция принудительного прерывания. Как отметил один наш эксперт, пожелавший

остаться неизвестным, этот вариант принудительного завершения разговора остался еще с тех времен, когда «сотовые аппараты стоили тысячи долларов и их основными покупателями были ребята в малиновых пиджаках, с бритыми затылками. Стоимость минуты была высока, и если в ежемесячном счете обнаруживались проблемы тарификации, то в сотовую компанию могли приехать «чисто конкретные пацаны» с «базаром» о том, куда ушли деньги». Сейчас ситуация с пользователями сотовых телефонов изменилась, но, несмотря на то что вероятность подобного «зависания» очень невысока, компании-операторы все равно устанавливают функцию прерывания длительного или «зависшего» разговора. По мнению некоторых экспертов, подобный порог принудительного отключения устанавливается, исходя из ряда параметров (операторы руководствуются массой самых различных аспектов работы с конечными потребителями на российском рынке) — одним из них вполне может быть усредненная продолжительность разговора по всем тарифным планам компании (в «одну кучу» мешаются pre-paid и безлимитные), которая умножается на 2 или на 3. Однако достоверной информации на этот счет нам обнаружить не удалось — пресс-службы на этот счет загадочно улыбались, а наши источники высказывали только предположения (самый распространенный ответ — «подобные исследования не проводились»).

Даже несмотря на некоторые спорные моменты, именно с этой точки зрения функция прерывания длительных разговоров в сетях мобильной связи выглядит вполне оправданной. Однако непонятным осталось следующее — как отметила **Елена Голикова**, Менеджер по связям с общественностью и маркетинговым коммуникациям компании Эрикссон,

Восточная Европа и Центральная Азия, «с точки зрения возможностей оборудования отключение звонка через определенный промежуток времени может устанавливаться как на сеть целиком, так и на отдельные группы. Однако окончательная настройка делается исключительно на основании решения оператора связи. К системе pre-paid рассуждение об отключении звонка после 30 минут разговора вообще неприменимо, так как здесь действует иной механизм — вы говорите, пока на счету остаются средства».

Получается, можно освободить от такой функции, скажем, безлимитных абонентов или определенные тарифные планы — однако операторы, кроме МСС, предпочитают выставлять ограничения на все типы звонков, даже на внутрисетевые разговоры своих собственных абонентов. В этой связи несколько озадачила позиция службы технической поддержки ЗАО СоникДуо — я обратился к ним с просьбой прокомментировать ситуацию с прерыванием связи. И вот среди прочей информации я получил достаточно любопытный текст: «Длительность входящего звонка ограничена 30 минутами по техническим причинам и не зависит от тарифного плана и от того, с какого телефона совершается вызов... Настройки используемого сетевого оборудования позволяют принудительно прекращать соединения большой длительности... Поскольку указанные настройки производятся при производстве коммутационного оборудования, в настоящее время между ЗАО «Соник Дуо» и поставщиком сетевого оборудования ведутся переговоры об изменении настроек».

Таким образом, для всех пользователей сотовых телефонов на поверхность «всплывает» не очень радостный факт — поговорить столько, сколько захочется, вряд ли возможно в принципе, любой оператор принудительно разрывает

соединение через определенный промежуток времени; хочется или нет, придется набирать номер снова. Самое неприятное в этом — факт, что никто абонентов об этом не предупреждает заранее, и им остается удивляться постоянным «сбросам» в процессе длительного непрерывного разговора. Причем оператора совершенно не волнует тип звонка (город-мобильный, мобильный-мобильный), насколько разговор важен (обычная болтовня или обсуждение деталей контракта), и будет ли одним из абонентов адекватно воспринят обрыв связи. Кстати, подвергнуться такой не очень приятной процедуре «обрыва» может каждый абонент — к примеру, час разговора с мобильного на мобильный МТС стоит 60 центов (при использовании тандема «Оптима + суперлюбимый номер»), а час разговора мобильный-мобильный в сети МегаФон — 1 доллар 80 центов (тариф О`Лайт). А уж совсем обидно безлимитникам, заплатившим по полтораста сотен долларов за возможность разговаривать без ограничений вообще (имеются в виду местные вызовы), — у них такой «обрыв» вызывает вполне прогнозируемую ярость. Ведь несмотря на уверения абонентских служб в том, что доля звонков с продолжительностью более 30 минут «не превышает 0,005 % от общего количества соединений», в абсолютном исчислении это все-таки тысячи прерванных разговоров.

Пиратские базы данных

Украденные базы с данными абонентов сотовых компаний стали появляться на рынке в начале 2000 года. В настоящее время ими торгуют уже открыто через Интернет и на

лотках, вместе с прочими компактами. Мы решили выяснить, каким образом такие конфиденциальные данные попадают на открытый рынок и чем это грозит пользователю.

Очень показательный случай произошел в Санкт-Петербурге, когда гражданка Новой Зеландии решила на время пребывания в Северной столице купить себе самый простой pre-paid от МТС. Все было вроде быстро — выбрали салон с фирменной символикой, определились с нужной тарификацией, почитали условия звонков в Европу — пришло время предъявлять документы. Посмотрев на неизвестный ему паспорт, молодой человек, подключавший абонентов, долго и пристально вглядывался в разные странички, а потом задал замечательный по природе вопрос: «А где здесь указана прописка по месту жительства?» — в итоге пришлось искать российский паспорт и покупать нужный ей контракт на другое имя. Эта небольшая зарисовка, комичная для любой страны Европы, показывает, что, не сообщив своего ФИО, адреса жительства и других интересных данных, к сотовой связи в России, как известно, подключиться сложновато. Только почему при покупке данного вида услуг гражданин обязан раскрывать так много данных? А в некоторых регионах особо ретивые продавцы не только требуют паспорт, но и проверяют прописку, и без, скажем, самарского адреса абонентом именно в Самаре никогда не стать.

Для людей, привыкших к нашей действительности, все эти вопросы не выглядят риторическими. Ведь возможность проконтролировать, занести в базу и так далее и тому подобное — такой ресурс без внимания оставить никак нельзя, так как последствия этого вполне предсказуемы. Базы данных сотовых компаний становятся товаром. И совсем не важно,

кто выступает их продавцом — главное, сведения сугубо личные становятся достоянием общественности.

В сети Интернет данный товар представлен, что называется, лицом — почти каждый день мне на почтовые ящики приходят манящие письма с предложениями купить самые последние базы операторов сотовой и фиксированной сети. Подобная информация не так безобидна, как кажется — к примеру, зная паспортные данные владельца, его дату рождения, можно провести любую операцию с телефоном, включая блокировку, намеренную смену тарифного плана с целью списания денежных средств, подключения ненужных услуг, запроса баланса — в конечном итоге это вполне может привести к лишению надежного средства связи. По чужим паспортным данным вполне можно зарегистрировать (здесь, конечно, нужен сговор с персоналом дилера) номер на ничего не подозревающего пользователя, которому потом придется разбираться с чужими счетами — особенно это неприятно при контрактной система расчетов, когда сначала разговор, а потом деньги.

Как отмечает **Игорь Шкляр**, юрист АБ «Д. Потоцкий и Партнеры», Конституцией РФ (ст. 24) установлено, что использование и распространение информации о частной жизни лица (информации персонального характера) без его согласия не допускаются. Согласно требованиям гражданского законодательства, включая законодательство о защите прав потребителей, в случае нарушения прав потребителя (заказчика услуг) исполнитель (оператор СС) обязан возместить потребителю убытки, вызванные таким нарушением, а равно, при наличии вины, компенсировать нанесенный моральный вред. Кроме того, заказчик вправе расторгнуть договор с оператором, отказавшись от его услуг. Помимо этого, зако-

ном установлена уголовная ответственность (ст. 137 УК РФ) за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации — штраф в размере до двухсот тысяч рублей.

Операторов тоже можно понять — они, конечно, принимают свои собственные меры безопасности. Как утверждает специалист службы по связям с общественностью ОАО Вымпелком **Артем Минаев**, «для того чтобы избежать утечки этой информации, с нашей стороны, доступ к базе с данными об абонентах строго ограничен, и каждый вход в систему контролируется дирекцией по безопасности компании». Аналогичное мнение высказывает пресс-секретарь ОАО МегаФон **Марина Белашева**: «Компания использует административные механизмы и современные аппаратно-технические средства безопасности информации, позволяющие надежно защитить сведения об абонентах и исключить утечку базы данных». По словам **Александра Маношкина**, ведущего специалиста по рекламе и связям с общественностью ОАО «Московская сотовая связь», «компанией разработана целая система мер, направленных на предотвращение несанкционированного доступа к внутрикорпоративным базам данных, актуальной информации по абонентской базе. Специальное программное обеспечение (firewall) надежно препятствует попыткам несанкционированного доступа к внутрикорпоративной информации извне (случаев взлома защиты не зафиксировано), для сотрудников компании введена "ролевая иерархия" доступа к информации, т. е. каждый конкретный сотрудник компании имеет доступ к актуальной информации

в соответствии с выделенной для него ролью — уровнем допуска».

Однако нет той защиты, которую невозможно было бы обойти изнутри компании (кроме всего прочего, ничем не ограниченный доступ к данным имеют сотрудники правоохранительных органов), и, несмотря на всевозможные меры безопасности, утечки информации все-таки избежать сложно. Мало кто устоит перед соблазном срубить «легкие деньги» за простую копию кучи файлов — сделать это, безусловно, очень сложно но, как показывает практика, все-таки возможно. Даже если подобных «сотрудников» и ловили, то меры воздействия, скорее всего, ограничивались тихим увольнением с занесением в «черный список» работников телекоммуникационной отрасли — по крайней мере, огласки таким делам не придают.

Чтобы снизить ценность подобных данных, операторы идут на широкое внедрение сервисов, с помощью которых абонент может узнать состояние своего счета и добавить новые услуги самостоятельно и без обращения в службу сервиса с озвучиванием своих паспортных данных — к примеру, в частных беседах сотрудники калл-центра ОАО Вымпелком признавались, что по инструкции не могут подключать новые услуги абонентам тарифных планов Би+, клиент все должен делать со своего телефона самостоятельно (правда, оказать помощь при затруднениях сотрудники всегда готовы). Кроме того, по информации службы безопасности МегаФон-Москва, в дополнение к паспортным данным, можно оставить в абонентской службе пароль, только при упоминании которого будут производиться все операции с номером телефона. Другой вариант — завершившаяся смена паспортов в конце 2003 года помогла владельцам телефонов изменить свои

данные в базе оператора, и теперь многим мошенникам сложно будет доставить неприятности законопослушным абонентам. Хотя, по признанию людей, занимающихся этим бизнесом, такое решение проблемы весьма недолговечно — только до очередного похищения базы.

Кстати, если абонент обнаруживает, что некто проделывает несанкционированные операции с его лицевым счетом, то по итогам расследования обычно принимается удовлетворительное для абонента решение — можно сменить номер телефона, можно воспользоваться паролем. Обычно эти вопросы требуют индивидуального подхода, и операторы не склонны их особо афишировать.

Кстати, на рынке предлагают базы почти всех известных операторов как фиксированной, так и сотовой связи — МТС, БиЛайн, Мегафон, а также компании МГТС, ПетерСтар и Северо-Западный Телеком, Delta, Fora. Типовой «комплект поставки» — это 1-2 CD с «родной» программой-оболочкой или хорошей программой Cronos в качестве оболочки (в развернутом состоянии на диске база данных занимает от 800 Мб до 1,65 Гб) для Windows 95/98/Me/NT/2000/XP. Есть разные версии программы — к примеру, «полная» включает в себя такие показатели, как ФИО, дата рождения, паспортные данные, адрес места жительства, ИНН, ОКОНХ, юридический адрес, контактный телефон (не мобильный), дата подписания контракта и прошедшие платежи, даты подключения и отключения телефона, адрес доставки счета, полная история по любому телефону с указанием всех владельцев или арендаторов. Есть и версия «лайт» — номер телефона, ФИО (как вместе, так и раздельно), дата рождения, адрес, наименование и ИНН юр. лица. Все ведет к тому, что источников «утечки» несколько — каждый из них поставляет информацию,

которую может взять в силу своих полномочий доступа. Стоимость программ — от 500 до 1500 рублей за каждый CD или комплект из двух дисков. Даты актуализации обычно не превышают квартала — «поставщики» работают весьма оперативно, очень быстро учитывая новые подключения операторов.

Однако «наколоть» при покупке незаконной информации могут даже покупателя. Первый способ, по мнению **Артема Минаева**, самый распространенный — дату актуализации мошенники проставляют любую, а вот само информационное наполнение системы старое. То есть пишем «октябрь 2003 года», а на самом деле версия базы, к примеру, от конца 2002 года. Еще пример: предложения о продаже баз МегаФон-Москва и БиЛайн-Москва (2003 года) являются мошенническими, и «на лотках» таких дисков нет (потому что продаваемый с лотка диск можно проверить на месте и обнаружить подлог). Как отмечает **Роман Проколов**, советник Генерального директора ЗАО «Соник Дуо», «для защиты абонентской информации в сети «МегаФон-Москва» используются современные аппаратные и программные средства. Кроме того, большую роль играет корпоративная лояльность персонала. Все эти меры на сегодняшний день доказали свою эффективность — наша база данных осталась, пожалуй, единственной базой, закрытой для пиратов и «взломщиков» — информация об абонентах сети «МегаФон-Москва» отсутствует в продаже». На лотках можно купить базу МТС Московского региона, актуальность базы — середина прошлого года, а также базы сотовых операторов Питера. Основанием для таких утверждений служит периодически проводимый мониторинг рынка баз данных силами служб безопасности операторов сотовой связи.

Есть и второй способ «сравнительно честного отъема денег» — как совершенно справедливо отмечает пресс-секретарь ОАО МегаФон **Марина Белашева**, «множество сайтов, которые предлагают такие базы, являются чистой воды мошенничеством, типичные признаки: анонимное общение с потенциальной жертвой (только контактные e-mail на анонимных бесплатных серверах), получение денег через анонимную систему электронных переводов «Яндекс-Деньги» или WebMoney, обещание выслать некие мифические коды доступа к CD с базами данных». Скорее всего, если приобретать похищенные базы по Интернет, авторы сайта никогда не пойдут на личную встречу с покупателем и сразу после получения денег перестанут отвечать на письма. Найти их, чтобы вернуть деньги, обычному гражданину обычно не под силу, даже милиции — слишком много таких преступлений, а незначительный ущерб (400–500 рублей) — не повод для полномасштабных боевых действий со стороны правоохранительных органов.

Случаи хищения баз данных происходят и будут происходить везде, где для покупки сотового телефона и/или контракта сотовой связи требуется показать паспорт. На пиратских рынках стран СНГ тоже можно найти нелегальные базы данных — продаются в уличных киосках наряду с паролями к порно-сайтам и платным «буржуйским» (на жаргоне хакеров) серверам. Из-за сравнительно небольшой (по российским и украинским меркам) базы пользователей во всех странах СНГ обычный лазерный CD может содержать все телефонно-адресные базы целого государства из нескольких операторов. Подобное вторжение в личную жизнь граждан вызывает у них самих, понятное дело, самые сильные эмоции. Но пересажать всех продавцов подобного товара

проблематично — «авторы» базы данных напечатают еще ровно столько дисков, сколько потребует рынок. Следовательно, остается уповать только на расторопность спецслужб, которые, по идее, должны узнавать о подобных «новинках» раньше журналистов. А также на проницаемость корпоративной защиты сведений самих сотовых операторов, без помощи сотрудников которых такая коммерческая «утечка» информации произойти бы не могла.

Мобильные сервисы безопасности

Чрезвычайная ситуация — это бег наперегонки с Судьбой. Мобильный телефон — зачастую та единственная «соломинка», которая может спасти человека из безвыходной ситуации, ведь его можно взять с собой практически куда угодно. Для многих пользователей мобильной связи возможность попросить о помощи в критической ситуации является основной причиной, по которой они покупают мобильный телефон. Однако на первый взгляд «ничего не выжать» из пусть самой совершенной, но все-таки сотовой трубки. Однако после знакомства с мобильными сервисами операторов понимаешь, что это совсем нет так.

Мобильный SOS

Исходящий вызов в службу спасения — это как SOS на море, его примут и передадут по назначению вне зависимости от того, зарегистрирован ли вызывающий телефон в чьей-

то конкретной сети или нет. Главное, быть в зоне действия любой сети своего стандарта (GSM, NMT, DAMPS или CDMA), и можно набирать телефон экстренного вызова. Как отмечают эксперты сотовой сети Сонет, «несмотря на то, что служба спасения — негосударственная коммерческая организация и ее поддержка не входит в социальную нагрузку при получении лицензии, все равно вызовы подобных служб абонентами полностью оплачивает оператор». А вот «вызовы по номерам экстренных служб 01, 02, 03, 04 — бесплатны для абонента потому, что являются условием предоставления услуг компанией-оператором», — добавляют сотрудники МСС.

Свои службы спасения есть в любом крупном городе России с населением свыше 500 тысяч человек — для их вызова стоит помнить короткие номера набора. Сотовая сеть «БиЛайн» — 911, «МегаФон» — 112, Мобильные ТелеСистемы — 112, Московская сотовая связь — 007, радиотелефонная сеть АСВТ «Алтай» — 999, сотовая сеть «Сонет» — 911. Кстати, если ближайшая базовая станция занята (слишком много абонентов), то вызов по экстренному каналу будет обработан с наивысшим приоритетом — он «сбросит» gprs-сессию (если тайм-слот, выделенный на это, запрограммирован динамически) или любой разговор (кроме абонентского номера со специальным приоритетом).

Кстати, службы экстренного реагирования были созданы и оперировали в европейских странах задолго до того, как появились сотовые телефоны. Еще в 1937 году Великобритания стала первой страной, которая создала и использовала универсальный номер для аварийных ситуаций. Эта единая телефонная система номера 999 использовалась полицией, пожарными и медиками. В Бельгии номер был 900, в Дании и

Австралии — 000, Швеции — 80000, Японии — 119, Новой Зеландии — 111. В 1959 году Канада также осознала пользу одного универсального номера для безотлагательной помощи и начала пользоваться британским вариантом (999), а чуть позже — 911.

В США идея создать универсальный номер помощи появилась в 1957 году. Крупнейший монополист, компания AT&T, избрала номер 911, потому что легко запоминался, и его можно было набрать довольно быстро — подобная комбинация цифр никогда прежде не использовалась в качестве телефонного кода или номера каких-либо служб. Технологическая адаптация номера также представлялась достаточно простой. С тех пор код 911 получил статус стандартного национального телефонного номера для всех экстренных вызовов.

В США существуют более 6 тыс. диспетчерских центров, принимающих звонки на номер 911. Большая часть из них оснащена специальной аппаратурой: когда звонок поступает в отделение, то телефонный номер и адрес звонящего сразу отображаются на дисплее оператора, что делает развертывание спасательной операции более оперативным. Это бывает особенно важно, когда звонящий страдает дефектом речи или просто не в состоянии говорить. Чтобы приехала полиция, пожарным и «скорой помощи» достаточно набрать номер и не выключать связь.

В России организация экстренных служб пока хромает. В городах с населением более 1 миллиона человек есть свои службы спасения. Вот для примера — только в одной Московской службе спасения, крупнейшей в России, работает около 400 сотрудников. Это не только спасатели, но и операторы связи, работа которых состоит в приеме и фильтрации

всех поступающих звонков, в большей степени с сотовых телефонов (у москвичей более 10 миллионов сотовых телефонов). В сутки обычно бывает до 30–40 тысяч обращений (в большей степени по мобильным телефонам) — просят вызвать «скорую помощь», пожарных или спасателей (для нестандартных случаев). Экипажи выезжают до 100 раз в день — помощь требуется не только людям, но и животным — спасают кошек, собак, а также крокодилов, экзотических обезьян и ягуаров.

В других регионах оператор организует переключение экстренных вызовов либо на МЧС, либо на милицию. Причем подобное положение вещей не устраивает ни сотового оператора, ни милицию или МЧС. Известно, что многие проверяют работоспособность своего «мобильника» при помощи звонка на 112. Часто в экстренных службах просто не обращают внимания на звонки с «мобильного» — положение печальное. Еще один вариант — переключение оператором вызова по номеру 112 на свою операторскую службу. Этот вариант хуже всего — надо прослушать всю рекламу оператора, и только после этого подключится «мобильная барышня». При этом в таких случаях операторы не подготовлены для решения оперативных вопросов и страдают отсутствием необходимых знаний.

Как это работает

Когда звонок с мобильного телефона поступает в диспетчерский центр службы спасения, в течение нескольких секунд на него отвечает оператор, называющий свой персональный номер. Звонящим рекомендуется запомнить этот номер: на тот случай, если обслуживание оператора вызовет какие

либо проблемы или недовольство и будет необходимо позже установить его личность. Оператор начинает задавать разнообразные вопросы, ответы на которые помогают ему классифицировать звонок, в зависимости от обстоятельств происшествия. Эта классификация внедряется в специальную компьютерную систему, которая устанавливает ближайшую милицейскую, санитарную или пожарную машину, которая сможет безотлагательно выехать на место происшествия. Каждый звонок также кодифицируется по уровню срочности. На первом месте по срочности — помощь, которую запрашивает сотрудник правоохранительных органов, находящийся при исполнении служебных обязанностей. Далее следуют: информация о совершающемся преступлении и серьезные проблемы со здоровьем. На последних местах по степени срочности вызова находятся сообщения об актах вандализма и плохом обращении с животными.

При звонке с сотового телефона рекомендуется сразу информировать оператора, какая служба необходима звонящему — милиция, служба газа, спасатели, пожарные или медики. Имеет смысл сообщить полную информацию о своем местонахождении, о деталях инцидента, о наличии огнестрельного оружия и о том, представляет ли данный инцидент угрозу для жизни, есть ли пострадавшие и в каком они состоянии. Однако одной из самых важных просьб к населению является то, чтобы звонящие не преувеличивали и не приукрашивали факты — очень многие абоненты именно так и поступают, считая, что в этом случае помощь прибудет быстрее.

Операторы службы 911 проходят специальную подготовку, но в России пока диспетчерские службы не оснащены специальной техникой для глухонемых, а перевод возможен, в

лучшем случае, только с английского. Невозможно и отсылать в службу спасения SMS с описанием инцидента или MMS с фотографиями места происшествия. Однако все опрошенные нами представители сотовых операторов единодушны во мнении — «как только у службы спасения появится возможность принимать и обрабатывать SMS или MMS, мы обязательно введем соответствующие сервисы и оповестим об этом наших абонентов». А в МСС позиция еще более оптимистична — там рассматривается внедрение ряда перспективных разработок (видеонаблюдение, позиционирование на местности, сотовая сигнализация и т. д.) на базе услуг новой сети СКАЙЛИНК.

Еще одна проблема, с которой сталкиваются специалисты экстренных служб — зачастую невозможно определить точное местоположение абонента. Если в мегаполисе, за счет хорошего покрытия базовыми станциями, можно определить более-менее точное место происшествия, то в сельской местности сделать это затруднительно (точность — несколько сотен метров). Помочь с решением этого вопроса смогут специальные телефоны — аналог уже предложен производителями в Японии. В Стране восходящего солнца решили оснастить все мобильные телефоны системой, которая позволяет определять их местонахождение с помощью спутника — причем власти давно настаивали на появлении таких устройств. Например, на случай обращения в полицию или скорую помощь. Однако законодательство запрещает компаниям мобильной связи разглашать сведения о местонахождении сотового телефона без согласия владельца. Поэтому в качестве компромисса решено оснастить телефоны специальной кнопкой — массовое внедрение таких устройств начнется в 2005 году.

Кстати, в 2005 году и в США будет возможно определить местонахождение человека, звонящего по сотовому телефону, с точностью 50–100 метров. Существуют два способа решения этой задачи. Первый предусматривает установление в телефонах чипа Системы Глобального Позиционирования (GPS), что позволяют засекать месторасположение звонящего с помощью космических спутников. Недостаток этого метода заключается в том, что стоимость телефонного аппарата увеличивается на $40–50, которые вынужден будет заплатить каждый покупатель телефона. Второе решение предлагает лаборатория Adaptive Systems Laboratory Калифорнийского университета, разработавшая специальное программное обеспечение и оборудование, устанавливаемое на ныне существующих антеннах сотовой связи. В этом случае расходы будут нести не пользователи телефонов, а компании-провайдеры. Ныне с сотовых телефонов в США совершается примерно треть всех звонков в службу спасения 911.

Экстренный вызов

Помимо голосового канала экстренной помощи есть и другие технические новинки. К примеру, в некоторых регионах России (в Москве — уже коммерческая эксплуатация) идут опытные испытания т. н. «кнопки экстренного вызова милиции». Суть сервиса проста — кнопка экстренного вызова милиции, вмонтированная в мобильный телефон, и позволяет в случае опасности срочно вызвать наряд сотрудников внутренних дел. В Москве сервис называется Мобильный телохранитель и предоставляется сотовым оператором МТС. В российских же регионах вполне могут быть использованы изделия управления технических средств объедине-

ния «Охрана» при МВД. Основная проблема — внедрить у местных операторов систему точного позиционирования через мобильные сети или взять на вооружение технологию спутниковой навигации GPS.

Основная цель данных разработок заключается в том, что человек, независимо от того, где он находится, может в течение нескольких минут в случае опасности «без лишних объяснений» вызвать помощь. После нажатия на кнопку сигнал о месте нахождения человека с помощью спутниковой системы поступает на пульт оператора объединения «Охрана», и по тревожному вызову на данное место выезжают сотрудники милиции.

Внимательные родители — еще одна благодатная категория сотовых операторов. Именно они являются большой целевой группой для сервисов под общим названием «Забота о детях». Уже в 2004 году федеральные сотовые операторы предложат (сначала, правда, в крупных городах), услуги на базе точного позиционирования. За счет хорошего охвата своими базовыми станциями российских мегаполисов всегда можно будет точно сказать, где находится ребенок с сотовыми телефоном — дома делает уроки или пропадает в игровом клубе. Ведь местоположение абонента будет указано графически — красная точка на карте, причем всегда можно будет прочитать адрес (название улицы, номер дома) и узнать, какие объекты (образовательные учреждения, развлекательные центры и т. д.) находятся в этом здании. Родитель должен будет активировать эту услугу у своего любимого чада, и по запросу система будет выдавать ему точные координаты несовершеннолетнего обладателя сотового телефона.

Для усиления безопасности своих автомобилей можно использовать систему WebLocator. Это интернет-система

диспетчеризации транспорта, использующая ресурсы сетей сотовой связи и GPS. В системе на современном уровне решены вопросы разделения прав доступа и информационной безопасности, используются последние достижения в области связи, реализуются передовые подходы в области управления транспортом (Fleet Management). Координаты автомобиля определяются с помощью 12-ти канального GPS-приемника, получающего сигналы от спутников. Кроме координат (широта, долгота) GPS-приемник также определяет скорость и направление движения. Данные координаты накладываются на компьютерную карту, по которой всегда можно понять, рядом с каким зданием и по какой улице сейчас едет машина. Точность определения местоположения борта определяется точностью используемых GPS-приемников и составляет от 10 до 25 метров. В городских условиях точность может иногда падать до 100–150 метров при проезде мимо высотных зданий, под высокими деревьями, под мостами или в тоннелях.

В качестве стационарно устанавливаемого бортового комплекта в настоящее время предлагается устройство Falcom A2D-JP3, позволяющее контролировать до 3-х датчиков и одно исполнительное устройство. Для мобильного бортового комплекта предлагаются сотовые телефоны с телематическими/GPS-функциями Benefon Track Pro 1.1 и Benefon ESC! NT 2002. Оборудование поставляется в комплектации, достаточной для полноценной работы. В дополнение, существует обширный список аксессуаров.

Однако кроме дополнительных «наворотов» для собственной безопасности можно использовать и традиционные сервисы. Как отмечает **Роман Проколов**, советник генерального директора «МегаФон-Москва»: «Мобильные сервисы,

связанные с безопасностью абонентов, будут развиваться в ближайшее время бурными темпами. К примеру, очень интересна в этом смысле технология MMS — если абонент попал в ДТП, всегда есть возможность, не откладывая, отправить в свою страховую компанию фотографии прямо с места происшествия. Встроенный фотоаппарат в сотовом телефоне способен уловить основные детали — повреждения автомобиля, участников ДТП, расположение транспорта относительно дорожной разметки и так далее. Причем отправить фотографии приемлемого качества можно сразу на электронную почту с текстовой версией случившегося». Дело в том, что любой спорный момент трактуется неоднозначно, а наличие фотографий является дополнительной доказательной базой, что в конечном итоге сэкономит абоненту время, потраченное на дальнейшее общение с сотрудниками ГАИ и страховщиками. Тем более что часто у милиции, как правило, нет с собой фотоаппаратов и кинокамер — все рисуется от руки на белом листке бумаги, здесь легко допустить отклонения от реальности.

Кражи мобильников

Колоссальное увеличение количества абонентов сотовых сетей за последнее время привело к тому, что проблемы, связанные с утратой мобильного телефона, приняли массовый характер. Телефоны теряют, телефоны воруют, наконец, нередко совершаются более тяжкие преступления: грабежи и разбойные нападения с целью завладения мобильным телефоном. Ведь мобильный телефон — не только средство

связи в современном городе. Это еще и очень дорогое электронное устройство — по стоимости многие модели сравнимы с хорошим цветным телевизором, современным DVD-плейером или стереосистемой. При этом сотовики обладают неоспоримым преимуществом для любого грабителя — они компактны по размерам и весу, не обладают никакой серьезной защитой и могут быть украдены множеством различных способов. Не удивительно, что сегодня грабежи сотовых телефонов по своему количеству превышают количество совершенных краж, в т. ч. из квартир.

Было и прошло

По официальной статистике начальника первой оперативно-розыскной части Криминальной милиции ГУВД Москвы **Дмитрия Чепчугова**, каждый день в Москве в среднем похищается около 50 сотовых телефонов. Но эти цифры отражают только количество людей, пожелавших обратится с официальным заявлением в правоохранительные органы — латентных преступлений на порядок больше, причем число грабежей у граждан сотовых телефонов постоянно возрастает.

Существует множество вариантов отъема средств связи у законных владельцев, но в общем их можно разделить на несколько основных категорий.

Обман — завладение имуществом происходит по наивности или непредусмотрительности самого владельца. Преступники с удовольствием эксплуатируют все добрые эмоции, которые вы можете испытывать к людям, которые обращаются за помощью. К примеру, Вы стоите в ожидании встречи с человеком в метро, на остановке общественного транспорта или

просто на улице, и к вам обращаются с просьбой дать сотовый телефон для экстренного звонка. Как только вы передаете аппарат человеку, он делает вид, что звонит, в процессе «разговора» начинает медленно отходить от вас, ловит момент и, в зависимости от ситуации, вскакивает в автомобиль с подельником, который скрывается в неизвестном направлении, или банально убегает.

Разновидность обмана — игра на доверии. В общественном месте (театр, кино, фаст-фуд) у вас просят позвонить телефон под предлогом, что у самого села батарея. «Симку» предлагают вставить свою, чтобы не тратить чужих денег. Нужного номера на телефоне не оказывается, и злоумышленник просит подождать, пока он сбегает с вашим телефоном до своего автомобиля и найдет нужный номер — свой телефон оставляет вам. Ожидание обычно затягивается до бесконечности — преступник бесследно исчезает, а оставленный в залог «телефон» оказывается отлично сделанным, красивым, но муляжом — почти не отличишь от настоящего.

Кража — воришки также быстро освоили новый рынок. Денег в кармане может быть немного, а вот сотовый телефон в столице есть у 60% жителей. Причем часто это дети, которые не смогут оказать внятного сопротивления. Мобильный телефон могут «порезать» вместе с сумкой, вытащить из кармана (особенно заднего) или срезать с ремня, если он закреплен там с помощью пластиковой прищепки, которые, кстати, легко ломаются. Больше всего проблем возникает с новыми моделями, которые весят менее 80–90 г и почти не ощущаются в кармане. Чаще всего крадут сотовые телефон в транспорте при большом скоплении пассажиров.

Разбой — иначе его еще называют «метод рывка». Как показывает практика, грабители выбирают своими жертвами

слабую половину человечества. Молодые красавицы, отдавая дань моде, носят свои мобильные телефоны на шнурке на шее, закрепляют их на поясах брюк и юбок. Сорвать такое «украшение» не представляет труда — соединительная прищепка выполнена из пластика и ломается от малейшего усилия.

Находка — иногда после кражи мобильный телефон сам быстро находит своего хозяина. Обычно в сотовом телефоне есть домашний и рабочий телефоны жертвы, а если вору не очень хочется связываться с перекупщиком, то через несколько дней предыдущий владелец аппарата услышит у себя звонок с предложением вернуть якобы найденный сотовый за половину стоимости. На встречу обычно приходят безобидные старушки, которые и отдают за деньги «найденные» сотовики. Доказать соучастие в преступлении в подобных случаях достаточно сложно, тем более что по закону «нашедший» вещь действительно имеет право требовать вознаграждения. Возврат якобы найденного телефона хозяину за вознаграждение — явление столь частое, что специалисты советуют потерпевшему самому прислать на свой номер (пока вор не выкинул SIM-карту) SMS-сообщение с предложением выкупить «находку».

Случаются проблемы и с самими правоохранительными органами. Бывают случаи, когда после проверки документов граждане не досчитывались своих мобильных телефонов. Как рассказала нам одна **собеседница на условиях анонимности**, «однажды на улице ко мне «подкатили» два «сотрудника с погонами» и задержали «до выяснения». Я только что купила себе новый телефон, а на старый документов не оказалось — покупала с рук. После моего «допроса» мне недвусмысленно намекнули, что необходимо «позолотить ручку», иначе телефон задержат до выяснения обстоятельств, и что

он, скорее всего, обязательно окажется «ворованным». Платить я наотрез отказалась, высказала все, что о них думаю, и в результате домой вернулась без телефона».

Поскольку этот способ «расставания» со своим мобильным телефоном достаточно распространен (судя по анализу тематических форумов), то прокомментировать ситуацию согласился юрист **Юрий Ермолов**: «В рядах правоохранительных органов время от времени обнаруживают «оборотней» — возможно, указанные сотрудники из их числа. Во-первых, прежде чем начинать любое общение с представителями правопорядка, попросите их предъявить служебные удостоверения и перепишите или запомните ФИО/должность/место работы — будет хотя бы, с кого спросить. Во-вторых, ни один милиционер не имеет права досмотреть Вас лично и ваши вещи без двух понятых и составления протокола. Сотовый телефон — частная собственность, никто не имеет права конфисковать личные вещи без санкции суда (ведь фактически был произведен обыск). Однако не стоит сопротивляться — проще успокоиться и потом написать аргументированную жалобу. Но протокол об изъятии получить, конечно, желательно. В-третьих, надо вести себя предельно корректно, т. к. «сопротивление при задержании» еще никто не отменял. После окончания общения с такими «милиционерами» звонить в УСБ МВД 2004703, 2002617, 2224717, а еще лучше везти заявление лично и регистрировать факт его подачи».

«Аппарат ушел, как дети в школу»...

Итак, сотовик срезали, вытащили или банальным образом отобрали. В таких случаях, как правило, сценарий один: из телефона стандарта GSM немедленно удаляется сим-карта

владельца, и он поступает в продажу на вторичный рынок, переживающий в настоящее время период бурного расцвета, пик которого еще не наступил. Так как производители сотовых телефонов сильно пострадали от упадка в мировой телекоммуникационной индустрии и больше не собираются демпинговать, выпуская все более и более дешевые аппараты, а количество абонентов в российских сетях стандарта GSM очень динамично увеличивается, то в скором времени неорганизованный вторичный рынок сотовых телефонов будет еще более массовым, чем сейчас. И хотя каждый абонентский терминал GSM передает при звонке свой уникальный номер (IMEI), без соответствующих законодательных актов добиться обязательной блокировки утраченных аппаратов в сетях российских операторов сотовой связи пока, к сожалению, представляется нереальным.

Светлана Сергеенкова, ведущий специалист службы по связям с общественностью ОАО «ВымпелКом»: «В компании ведется обработка и учет всех заявлений, обращений наших абонентов (как устных, так и письменных), связанных с утратой/кражей телефонов. Компания сотрудничает с правоохранительными органами в полном соответствии с действующим законодательством». Однако отключать украденные сотовики, если они появляются в сети, политической воли пока нет. Сходная ситуация и на Кавказе — как отметила **Ольга Дюкова**, пресс-секретарь ОАО «Мобиком-Кавказ», «список IMEI по украденным телефонам мы, к сожалению, не вели с самого начала существования сети — ведь создание и актуализация подобного списка телефонов имело бы смысл в случае общеобязательности данной процедуры. Если в Москве главные офисы соберутся и решат совместно действовать в этом направлении, то мы обязательно присоединимся. А сей-

час обращения от парвоохранительных органов с целью установления IMEI похищенных телефонов, конечно, есть — необходимую информацию мы предоставляем».

Но есть и другие примеры — **Владимир Волков**, специалист по PR ЗАО «Мобиком-Центр», рассказывает о другой ситуации: «Мы совместно с органами внутренних дел ведем постоянную работу по выявлению телефонов, украденных как у абонентов сети МегаФон, так и у абонентов других компаний. У нас существует база данных по IMEI сотовых телефонов, которые были украдены у абонентов компании. IMEI сотовых телефонов вносятся в базу по запросу ОВД — в неделю поступает до 70 запросов».

В **пресс-службе Северо-Западного филиала ОАО «МегаФон»** нам рассказали, что до января 2003 года компания практиковала ведение «черных» и «серых» списков. Абонент мог написать заявление в милицию, обратиться в центр обслуживания, и его телефон попадал в «серый» список, т. е. при регистрации в сети Северо-Западного филиала ОАО «МегаФон» он мгновенно отслеживался службой безопасности. При занесении телефона в «черный» список подключение его к сети «МегаФон» на Северо-Западе становилось невозможным. Но после того, как на рынок вышли другие операторы, которые на сегодняшний день не поддерживают практики ведения «черных» и «серых» списков, инициатива компании стала бессмысленной. Однако людям, попавшим в неприятные ситуации, по-прежнему помогают. К примеру, в центрах обслуживания Северо-Западного филиала ОАО «МегаФон» можно получить наклейку, которую помещают на аккумулятор телефона, указав на ней контактную информацию владельца. Это увеличивает шансы возврата телефона хозяину, по крайней мере, в том случае, если он

был не украден, а потерян, и был найден человеком с добрыми намерениями.

Но есть и более интересные решения. **Ольга Сафаргалиева**, руководитель по связям с общественностью ЗАО «Уральский Джи Эс Эм»: «База утраченных IMEI не ведется — ведь с украденным аппаратом можно подключиться к сети другой сотовой компании в любом регионе, стандарт GSM в России весьма распространен. Однако в связи с участившимися обращениями абонентов по поводу кражи/утери телефонных аппаратов с 16 сентября 2003 года мы ввели в опытно-коммерческую эксплуатацию услугу «Дата последнего вызова». Данная услуга предоставляет абонентам нашей сети, потерявшим телефон, узнать, используются ли их телефоны в сети». Услуга предоставляется по заявлению абонента при наличии документа, удостоверяющего личность. Отчет абонент может получить на следующий день после написания заявления лично в Центре Обслуживания «МегаФон» или по электронной почте, указанной в заявлении. Предоставляется информация о дате и времени последнего зарегистрированного в сети вызова; типе вызова (исходящий/входящий) и регионе, с территории которого этот вызов был совершен. Эта услуга устанавливает лишь факт использования телефонного аппарата с определенным серийным номером в сети «МегаФон» ЗАО «Уральский Джи Эс Эм». Информация о местонахождении трубки, номерах, с которых и на которые с нее звонят, а также о том, кто использует украденный телефонный аппарат, предоставляется только по запросу сотрудников МВД РФ.

Тем не менее, некоторые действия для минимизирования ущерба можно предпринять. Если телефон похищен, и в этом

есть твердая уверенность (его можно, к примеру, выронить без злого умысла), то необходимо писать заявление в милицию. Там вам, конечно, могут выставлять препоны — оперативники в «дружеских» беседах будут рассказывать, что найти телефон сложно и не стоит с этим связываться, но если будете тверды, то заявление принять обязаны. Сразу после этого, если вы точно знаете, где было совершено хищение, есть возможность поездить с дежурным экипажем ППС по району с целью опознания злоумышленников. Стоит учесть, что по новому УК заводить уголовное дело милиция обязана, только если рыночная стоимость похищенного превышает 5 МРОТ (3000 рублей), а многие бэушные мобильники стоят дешевле — хищения на меньшую сумму являются административными правонарушениями.

Одновременно стоит позвонить по справочному телефону своего оператора сотовой связи и заблокировать sim-карту. Для этого достаточно устного заявления с указанием паспортных данных — дубликат sim-карты и окончательную блокировку предоставят только на основании письменного заявления, для этого даже не обязательна справка из ОВД о возбуждении дела по факту кражи или разбойного нападения. По опыту операторов сотовой связи, сотрудники правоохранительных органов часто просят их выявить звонки с украденных телефонов или определить примерное местонахождение мобильника. Если запрос оформлен в соответствии с законом, в рамках следственного дела специалисты могут это сделать. Но чаще всего эти следственные действия проводятся в связи не с кражей мобильного телефона, а с квартирными кражами или разбойными нападениями, в ходе которых был похищен и аппарат мобильной связи.

Странное слово IMEI

Многие полагают, что, как только вор выкинул из аппарата SIM-карту (а именно так и делают), обнаружить телефон невозможно. Специалисты утверждают, что это не так. Каждый мобильный телефон имеет свой уникальный заводской номер — IMEI. Его можно увидеть на задней крышке телефона под батарейкой. Этот номер «зашит» в программное обеспечение аппарата и сообщается на базовую станцию оператора при регистрации аппарата в сети или при совершении звонков. Поэтому, даже если в украденном аппарате поменяли карточку, телефон все равно можно найти. Вопрос — будет ли этим кто-либо заниматься всерьез? Ответ — вряд ли. Сначала мировой опыт — вот в Голландии компании сотовой связи рассылают на похищенные телефоны (их определяют по IMEI-номеру) сообщение «Этот телефон украден» раз в 3 минуты. В Испании, чтобы блокировать украденный или потерянный «мобильник», его законному владельцу достаточно позвонить оператору и сообщить 15-значный номер идентификации аппарата. Во Франции и в Австралии существует единый реестр всех украденных номеров, и любой оператор сотовой связи обязан немедленно заблокировать аппарат, который значится в «черном списке».

Попытки составлять списки краденых телефонов в Интернете делались и у нас. Такой реестр есть в Москве, есть свои списки в Петербурге и Екатеринбурге, где любой пострадавший может «объявить в угон» телефон, если он обладает необходимыми документами. Однако попытки перевести этот «чисто академический» интерес в реально действующий механизм у операторов пока, к сожалению, по-

терпели неудачу. **Павел Виг**, председатель совета Общества Пользователей Мобильной Связью: «Еще в 2002 году у нас были попытки установить с операторами взаимопонимание с целью создания базы по утраченным IMEI. Переговоры были проведены с господином Прянишниковым и господином Сусовым — однако дальше декларации дело не пошло. В МТС просчитали затраты и выяснили, что внедрять такую систему по своей инициативе не выгодно — а политической воли для этого пока нет. К сожалению, внести пункты об IMEI в действующий закон «О связи» мы не успели, теперь остается надеяться только на поправки».

Надо отметить, что правоохранительные органы не очень любят заниматься кражами мобильных телефонов. Средняя стоимость «мобильной игрушки» — $100, этого достаточно для возбуждения уголовного дела, однако глобальными результатами с положительной динамикой не может похвастаться ни одно УВД. И дело даже не в технической безграмотности — в милиции сотрудники все грамотные, про IMEI и сами знают, однако ответ потерпевшему всегда прост: «Мы, конечно, постараемся, но гарантировать ничего не можем». И тому есть одна причина — организационная. Ну просто не существует единой базы данных IMEI, которые украдены у абонентов. Хотя создать такую базу под эгидой, скажем, Ассоциации GSM в России не очень сложно — достаточно простого ведомственного распоряжения операторам, технические мощности у которых вполне для этого существуют. Ведь все операторы обязались содействовать правоохранительным органам, так записано в лицензиях. Правоохранительные органы могли бы пожелать, чтобы операторы им такое содействие оказывали, причем воззвать через Ассоциацию, которая, при желании, найдет способ это пожелание реализовать.

Как вариант и дополнение к базе, можно издать закон о запрещении обслуживания телефонов, чьи IMEI указаны как похищенные.

Еще один вариант подсказали специалисты сотовых операторов — в любом случае основой будет некоторая база данных (IMEI телефона, данные владельца, где и когда был похищен, какое УВД ведет дело о краже, разбое или т. д. — то есть кому звонить/писать по этому поводу), но вести ее будет один, так сказать «базовый» или «системный» оператор. Получение номеров будет поставлено по официальному каналу напрямую от правоохранительных органов, а остальные сотовые провайдеры и дилеры будут подключены к этой базе по зашифрованному каналу с ограниченными правами доступа — основную информацию смогут только читать, и если будет обнаружен аппарат с ворованным IMEI, то добавлять в соответствующие поля информацию о контактных данных владельца номера с которым такой сотовик «вышел на связь». Но быстро это сделать не получится — нужно соответствующее ПО и схема взаимодействия с ФСБ, так что полгода — это более реальный срок. Хотя, как и в первом варианте, остается вопрос политической воли — быть может, причина неустроенности вопроса о кражах мобильных телефонов в том, что организационные меры выгодны гражданам, а «государственным» людям на местах и, в конечном итоге, власти — толку от этого совсем никакого, только лишние «заморочки».

Есть, конечно, аргументы против ведения подобных баз. Как рассказал нам специалист по «перепрошивке» сотовых аппаратов на условиях анонимности, «работая в данной области, хочется отметить, что серийный номер телефона на 90% аппаратов поменять так же просто, как закачать новую

картинку — стоит это порядка $15. И люди, торгующие ворованными телефонами, имеют эту возможность. Вдобавок многие продавцы б/у не заморачиваются легальностью аппаратов — это траблы клиента». Однако стоит отметить, что сейчас производители озаботились этой проблемой, и для того, чтобы поменять IMEI, нужно перепаять микросхему. К тому же, если будет закон о наказании за перепрошивку IMEI (к примеру, в Австралии за такие «художества» дарят 2 года в местах не столь отдаленных, в Великобритании — 5 лет), то это все повернется совсем в другую сторону.

Выводы, к сожалению, пока неутешительны. Во-первых, чего только не придумывали талантливые инженеры для того, чтобы сделать украденный мобильный телефон бесполезным — предлагали ставить датчики для отпечатков пальцев на задней панели, встраивать механизмы для дистанционной блокировки или уничтожения телефона, создавать и пополнять базу украденных IMEI сотовых телефонов, засыпать ворованный мобильник sms-сообщениями и т. д. Но ничего должным образом не помогает — мобильники продолжают воровать сотнями тысяч. Поэтому самая адекватная защита в руках владельца сотового телефона — надо быть просто внимательным. Во-вторых, сотовый телефон не стоит носить в кармане широких джинсов, в карманах куртки, на шее на шнурке, в сумке, в барсетке. Трубка всегда должна быть рядом с рукой и в то же время не на виду. Самое оптимальное — носить в поясной сумке, ее из-под одежды очень сложно достать, так как она имеет жесткий металлический фиксатор, а нащупать рукой сотовую трубку всегда можно. И, само собой, не надо быть очень жалостливым и давать всем позвонить. Так никаких денег (на покупку новых телефонов)

не хватит. В-третьих, если вы решили защитить свой телефон с помощью страховки (стоимость годового полиса составляет 4,5–5% цены нового аппарата), стоит внимательно читать договор — в абсолютном большинстве случаев фирма-страховщик гарантирует возврат средств, только если телефон был украден из закрытого помещения. Если срезали с пояса — ваши проблемы.

Ваш номер больше не обслуживается

Множество абонентов жить не может без pre-paid тарифов — они по сути созданы для оперативных звонков, когда на первый план выходит быстрота реагирования, а никак не экономичность. Все уже знают, что любой тариф семейства Джинс, Би+, Лайт без абонентской платы, новую sim-карту можно купить буквально за 3–5 минут (иногда даже и без паспорта — как повезет), пополнить счет картами предоплаты. В общем — относительная простота для мобилизованного абонента, минимум бумажной волокиты и предельно ясные правила игры. Однако с точки зрения операторов pre-paid"ники — абоненты хоть и желанные, но не сильно выгодные. Можно было бы спокойно жить, зная, что у них низкий ARPU (в пределах 10–12$) и выговаривают они не очень много минут, постоянно звонят в абонентскую службу с просьбами подключить новые услуги или отключить надоевшие (для этого все «федералы» создали разветвленные системы электронного управления счетом и услугами — только чтобы операторов на это нудное дело не отвлекали).

Но pre-paid"ники еще и обладают «низкой лояльностью» — поговорят месяц-другой и sim-карту выкинут. Мало того что дилеру за таких «красавцев» оператор платить должен (правда, сейчас комиссию значительно срезали и будут выплачивать в рассрочку), но и в отчетности их потом упоминай и учитывай (аналитики за эти «мертвые души» операторов не сильно любят). Правда, против этого придумали тоже хороший «финт ногами» и ввели срок действия sim-карт — если определенное время абонент не совершает по своему номеру платных звонков и не отправляет sms, то его номер перестает обслуживаться. А еще операторы практикуют «сроки годности» на активацию sim-карт тарифов pre-paid — ее надо активировать (то есть начать использовать) в течение 30–90 дней с момента приобретения.

Все было бы ничего и так бы и жили абоненты и операторы без сильной взаимной любви и ненависти, однако в каждой хитроумной схеме бывают свои подводные камни. И один из них — остатки по счету. Схема проста — купил абонент карту предоплаты в 5, 10 или 20 (самые распространенные номиналы) долларов, а поговорил на 80–90% оплаченного времени, ну еще несколько sms-ок послал (всего на 95% оплаченного времени), а 5–50 центов или 1–2 доллара на карте остались. Про номер он забыл или карту затерял, и через положенное время оператор счет закрыл. Деньги, пусть небольшие, оператор получает, видимо, в награду за терпение. С точки зрения обычного абонента суммы не принципиальные, но абонентские базы у операторов растут, количество pre-paid sim-карт в продаже меньше не становится, и весьма изрядное «салями» (так на жаргоне называют мелкие остатки по счетам) перепадает операторам весьма регулярно. Деньги приходя,т а услуги связи по ним не оказываются — это

происходит по воле абонента, но факт остается фактом. По сути это безвозмезный подарок оператору.

В случае с МегаФон-Москва срок действия sim-карты — 30 дней. В случае, если на протяжении 30 дней с момента отключения телефона вы не активируете новую карту, ваш номер будет аннулирован, а остаток на счете («баланс») обнулен. По условиям договора «остаток денежных средств при этом не возвращается».

Элдар Разроев, комерческий директор «Мегафон-Москва»: «Существующие правила установлены не случайно — ведь у большинства операторов средние остатки по заблокированным sim-картам составляют менее 2-х долларов, а в подавляющем числе случае — несколько центов. Относительно больших (10–50$) остатков на счету: это, на мой взгляд, фантастика — за 30 дней можно определится, что с этими деньгами делать, ведь не просто так их «забрасывали» на этот счет. Как правило, люди обнуляют баланс до минимальной суммы звонка и выбрасывают sim-карту. Возможности вернуть эти деньги абоненту или перевести на другой мобильный счет у pre-paid абонентов нет. Это нормальное явление для любого сотового оператора, оно определяется технологическими особенностями препейд-платформ и учетной политикой. С контрактными абонентами вопрос решается иначе. Они обслуживаются с помощью билинговой системы, которая хранит историю платежей и может дать информацию о сумме неизрасходованных средств. И в случае расторжения контракта эти абоненты могут получить назад деньги, оставшиеся на балансе».

Компания МегаФон-Москва как-то уж очень жестко относится к своим pre-paid абонентам — к примеру, вводя вместо «бесконечных сроков платежей» платные «карты

продления». Возможно, за этот счет консолидируется абонентская база, и в итоге остается мало «мертвых душ» и образуется значимое количество платежеспособных клиентов, но не секрет, что отключенные таким образом абоненты достаточно трепетно относятся к своим телефонным номерам и такое быстрое блокирование вызывает естественное недовольство.

В МТС-Москва ситуация несколько другая — карта здесь активна в течение 180 дней, и по истечении этого срока, если абонент ни разу не сделал платных звонков или не отправлял sms (бесплатные звонки в службу сервиса — не в счет), то его счет также закрывают. Столь длительный промежуток времени установлен, исходя из модели поведения pre-paid абонентов, и соответствует мировому опыту. Однако (внимание!) при расторжении договора абоненту возвращается разница между суммой денежных средств, уплаченных им по настоящему договору, и стоимостью оказанных услуг.

Снять оставшиеся средства на sim-карте абонент может по следующей схеме: приехать в один их офисов комплексного обслуживания МТС, написать заявление о расторжении контракта и по истечении 15 дней приехать туда же или в другой офис (адрес всегда могут подсказать в справочно-информационной службе или в офисах) для получения остатка по счету.

Перенести остаток на другой активный счет нельзя.

Как нам рассказали **в пресс-службе МТС**, если абонент захочет восстановить свой номер, он может заключить новый контракт на любой из тарифных планов Единой системы тарифных планов МТС (т. е. не ДЖИНС). При этом нужно оплатить услугу выбора «внеочередного» номера, и тогда можно вернуть старый номер, если он окажется к этому

моменту свободным. Впоследствии абонент может поменять этот тарифный план обратно на ДЖИНС. Заключать новый контракт сразу на ДЖИНС нельзя по той причине, что тарифы этой группы не имеют услуги «выбор номера».

В случае БиЛайн-Москва sim-карта активна в течение 180 дней, в течение последующих 6 месяцев номер находится в «освобожденном» (термин специалиста call-центра Вымпелкома) состоянии — в свободную продажу он не поступает, но восстановить его абонент может, надо только пополнить счет на минимальный номинал карты предоплаты (5$). По истечении первых 180 дней есть возможность денежные средства вернуть — достаточно написать заявление, они никуда не «испаряются».

Дело в том, что если пропали деньги мелкие и незначительные, абонент вряд ли будет переживать. Другое дело ситуации, когда люди покупают карту pre-paid тарифа, регулярно «подкармливают» ее деньгами, хотя и не выговаривают много времени и через какое-то время кладут ее на полку или забывают об ее существовании. В первом случае чаще всего отмечаются пенсионеры, которым сотовик нужен на время дачного сезона — обычно сотовый телефон и номер им покупают взрослые дети, которые хотят таким образом телефонизировать своих родных. Они не очень сильно разбираются «в тонкостях этой штуки без проводов» и обычно очень обижаются по всем финансовым вопросам. Во втором — командировочные граждане, приезжающие в какой-либо регион по личным или служебным делам. И еще один вариант — это люди, у которых несколько мобильных номеров — при этом они находятся в крупном мегаполисе и какие-то номера используют как основные, какие-то как рабочие или только для личных

звонков. При незнании правил на таких счетах могут «сгинуть» и 10, и 20, и даже 40 долларов.

Однако в данном случае все не так однозначно. Например, закон знает понятие неустойки как меры ответственности за нарушение обязательств. Поэтому, предположим, что это могло бы быть похоже на неустойку (штраф), но тогда возникает вопрос: пользоваться мобильной связью — это обязанность или право абонента? Ответ понятен. Абонент вправе использовать мобильную связь и обязан ее оплачивать. Следовательно, неустойка может быть установлена только за неоплату, но не за неиспользование.

Игорь Шкляр, юрист адвокатского бюро «Д. Потоцкий и партнеры»: «Пользоваться телефоном — это право абонента. По договору об оказании услуг у абонента есть только одно обязательство — оплатить услуги (ст. 779 ГК РФ). А деньги снимать с остатка — это нехорошо. Это может быть квалифицировано как обременительное условие, грубо нарушающее права потребителя. С другой стороны, оно устанавливается по соглашению сторон. Однако в последнем случае это весьма слабый аргумент для сотовой компании. Я думаю, что здесь не только злоупотребление правом, но и даже присвоение чужого имущества (денежных средств). Подобное условие как обременительное может быть исключено судом из текста договора, заключение которого, как правило, происходит путем присоединения абонента к стандартным условиям».

Таким образом, вполне может найтись недовольный абонент, который из-за 10 центов организует индивидуальный или коллективный иск к оператору. Совсем не из-за желания вернуть свои деньги — просто это удобный политический инструмент, который, как и ружье на сцене театра, в течение

спектакля обязательно выстрелит. Подобная «мина» всегда может взорваться — причем, по законам жанра, в самый неподходящий момент. Вроде технически не очень сложно постулировать возврат средств абонентам в автоматическом режиме — путем перевода на другой мобильный счет, или возврат наличными через офисы компании. Ведь в этом случае тот самый определенный процент активных и недовольных рассосется сам собой — просто исчезнет сама проблема. Возвратов денег будет, безусловно, меньше, чем кажется, — можно создать сложную процедуру истребования остатков, но саму возможность предусмотреть все равно желательно.

Sim'ки уходят «налево»

Контракт в сотовой связи — святое дело. Именно эти условия являются основополагающими при взаимодействии оператора с абонентом. Как и во всяком юридически стройном документе, там присутствуют реквизиты сторон, которые несут обязательства по исполнению соответствующих условий. Но время от времени находятся «умельцы», которые преодолевают законные способы подключения, и тогда контракты получаются «левыми» или «липовыми» — данные, указанные в документе, могут быть не только неправильными, хуже, когда все оформляется на совершенно постороннего человека, который в один «прекрасный миг» обнаруживает, что должен сотовому оператору сотни долларов.

Всю проблему можно разделить на несколько основных частей.

Вопрос первый — можно ли законным способом приобрести контракт у оператора сотовой связи без заполнения контракта? Оказывается, да — это случается. К примеру, электронные автоматы IBox торгуют комплектами GSMLite без предъявления каких бы то ни было документов — только заправьте деньги в приемник купюр. В супермаркетах можно купить тарифы О"Лайт и Просто от компании МегаФон. А вот купить любой другой pre-paid без документов легально невозможно — никакой дилер обычно на такое не пойдет. Хотя на любом радиорынке спокойно можно купить без оформления не только Би+Тайм, и всевозможный Джинс в ассортименте, но даже тарифы контрактные — Оптима, Лайн. Там, видимо, все оформлено «честь честью» — у абонента просят только деньги, никакого паспорта.

Вопрос второй — можно ли при покупке контракта указать неверные и неточные данные? По действующим правилам, заключение контракта без оригинала паспорта невозможно. Однако субдилеры игнорируют эти правила. Чтобы рассмотреть ситуацию подробнее, мной был проведен «следственный эксперимент» — выбрав в Интернет первый попавшийся виртуальный магазин по продаже контрактов, я заказал себе (совершенно наобум) «Прием Дружеский» от МегаФон-Москва. Часа через три в дверь позвонили, и на пороге предстал куда-то спешащий курьер с всклокоченными волосами, который молниеносно заполнил бумаги, причем даже не попросил паспорта или его ксерокопии — все было записано с моих слов. Вручив мне часть самокопирующегося бланка, он так же стремительно исчез, оставив мне заветный картонный пакет с sim-картой и справочником абонента. Однако данные, которые я ему сказал, были несколько неточны — я сделал ошибку в номере и серии паспорта, однако это уже

никому не важно (во всяком случае, до первого личного обращения в офис оператора). Карту активировали в течении пары часов без всяких вопросов — дилер «на том конце провода» тоже не попросил никаких удостоверяющих документов.

Кстати, есть и, как говорится, оборотная сторона медали — она не слишком распространена, но все-таки встречается. Вот, к примеру, в интернет-форумах люди продают контракты с выгодным соотношением — за 44$ предлагается тариф «Дружеский» от Мегафон-Москва, на счету там 59$ (или за $5 предлагается контракт МТС, где на счету $15). Люди заказывают по сети Интернет и покупают — даже ехать никуда не надо, привезут, куда скажешь. А после посылают по факсу письмо с просьбой закрыть счет и через неделю-две забирают деньги. В случае с данным тарифом от МегаФона 15$ чистой прибыли гарантировано.

Как прокомментировал наш собеседник, на условиях анонимности «подобный «бизнес» может приносить 150–200 долларов ежемесячно. Объявления «жертв» я просматриваю в газете «Из рук в руки» или на сайтах типа «Сотовик». Мои паспортные данные известны только оператору, а мелких дилеров много — поймать меня невозможно. Главное не просить больше 2 контрактов сразу, лучше потом еще раз. И самое главное — все абсолютно легально. Со стороны выглядит просто — не понравился человеку тариф, взял и расторгнул контракт».

Кстати, никакого «игнора» у оператора для таких «расторженцев» не предусмотрено — ведь контракт заключается официально, доказать подвох в данном случае сложновато. Дилер самостоятельно увеличивает сумму на счете за счет своей дилерской комиссии для привлечения вни-

мания потенциальных покупателей — «за язык» его никто не тянет. Подобные потери пока, к счастью, не измеряются сотнями тысяч долларов упущенной прибыли — дилер просто покрывает этот убыток за счет получения дилерского вознаграждения за активных абонентов. Но за закрытый таким образом контракт дилер уже ничего не получит, некоторые «федералы» даже штрафут провинившихся таким образом продавцов, однако финансовые санкции наступают только в случае превышения определенного процента «левака».

Конечно, крупные дилеры имеют кроме базы своих клиентов еще и т. н. «черные списки» — это всевозможные кидалы, излишне придирчивые абоненты и мошенники, специализирующиеся на обмане в услугах сотовой связи. Таких, безусловно, не подключают. Этими списками обмениваются на паритетной и регулярной основе — взаимная помощь в данном случае оправдана, несмотря на жесткую конкуренцию.

Вопрос третий (основной) — откуда же берутся «левые контракты», по которым задолженность требуют у ничего не подозревающего абонента? Такие контракты — следствие высокой дилерской комиссии, когда оператор за привлеченного абонента платил продавцу единовременно сумму, эквивалентную $30 и даже $50. Конечно, заполнить несколько «липовых» заявлений в таком случае дилеру труда не составляло — живые деньги образовывались на счету очень быстро. Паспортные данные для таких «операций» брались из различных баз данных, которые сейчас в большом количестве продаются по всей Москве.

В основном «левые» контракты предлагают через Интернет — это спамерские рассылки, которые часто приходят в

ваш почтовый ящик, и форумы на популярных интернет-сайтах (кстати, их владельцы часто и не знают, что на этих страницах орудуют мошенники — всех не проверишь). Способы наиболее дешевые и массовые — за счет такой «ковровой бомбардировки» 1–2% откликов от отосланной рекламы такие «продавцы», конечно, получают. Однако это совсем не все — много «левака» можно найти на всевозможных стикерах и приклеенных бумажках в метро, на остановках общественного транспорта — если видите лозунги типа «БЕСПЛАТНОЕ подключение!», «Выгодные контракты сотовой связи!», «Подключу всех!», то это как раз такие господа.

Пережив пик «левака» в 2003 году, сотовые компании приняли свои меры противодействия, и волна незаконных подключений медленно, но пошла на спад. Этому есть несколько причин. Во-первых, дилерский рынок стабилизируется и плавно переходит от «дикого» во вполне вменяемое состояние. Во многом этому способствует политика сдержек и противовесов — теперь дилерская комиссия за подключенного абонента выплачивается не единовременно, а пролонгируется в течении нескольких месяцев и увеличивается от ARPU абонента и того тарифа, на который он был подключен. Во-вторых, у каждого оператора существует достаточно разветвленная система контроля своих продавцов (называются эти системы по-разному, — к примеру, в БиЛайн — это «Дилер on-line), по которой можно оперативно проверить, кто и когда подключил конкретного абонента, выражающего неудовольствие по поводу несправедливых начислений, и задать ему «строгача» в виде штрафа за несоблюдение условий дилерского соглашения. В-третьих, рынок близок к насыщению, и дилеры заинтересованы в долговременном сотрудничестве

с операторами, а потому стараются не разбрасываться субдилерством направо и налево, «лишь бы впарить».

Были ужесточены и меры безопасности. **Элдар Разроев**, комерческий директор «Мегафон-Москва»: «Оформление «левых» контрактов на паспортные данные уже действующих абонентов сети в нашей сети пока не зафиксированы. Связано это с адекватной политикой по отношению к дилерам, которая действует в нашей компании, и эффективной работой службы безопасности. В любом случае, если у абонента есть сомнения в своих счетах, все решается в службе кредитного контроля — достаточно прийти в офис и написать заявление с изложением фактов. Остальное — наши проблемы, решение будет найдено быстро. Мы не просим абонента доказывать, что он «не верблюд».

Кроме того, был проведен «апгрейд» биллинговых систем — теперь невозможно получить сколь-нибудь значимый отрицательный баланс (сумма обещанного/условного платежа рассчитывается, исходя из истории платежей конкретного абонента), а перетекание средств с одного лицевого счета на другой, пусть они и оформлены на одно лицо, невозможен. **Артем Минаев**, специалист по связям с общественностью ОАО «Вымпелком»: «Даже если дилер подключит нелегальным образом нового абонента на имя уже существующего, то последний не понесет финансовых убытков. В случае с абонентами, подключенными по кредитным тарифным планам, обман раскроется при неоплате ежемесячного счета, а абоненту достаточно будет сообщить о том, что ему не принадлежит тот или иной номер. В случае с абонентами, подключенными по тарифным планам «Би+», все тоже под контролем — наша платформа pre-paid не позволяет «уходить в минус». Соответственно тот, кто подключился на имя друго-

го абонента, сможет воспользоваться связью только на ту сумму, которую оплатил сам».

Вместе с тем, если вы оператор оператора с небольшой абонентской базой, то шанс попасть «на карандаш» к мошенникам незначителен — в таких фирмах любое аномальное поведение заметно сразу. **Александр Маношкин**, ведущий специалист по рекламе и связям с общественностью ОАО «Московская сотовая связь»: «за 2003 год было не более двух случаев оформления контрактов по подложным паспортам граждан РФ. Информация передается в службу безопасности компании, далее в органы МВД. Еще один аспект безопасности — через дилера не имеется возможности заключить контракт с МСС на уже существующий лицевой счет».

Однако если вам все-таки пришло грозное письмо от провайдера с общим смыслом «оплатите», а этот номер вы видите первый раз в жизни, то все можно решить быстро и мирно. Придется, конечно, посетить ближайший офис оператора и в службе финансого контроля написать заявление о том, что ничего общего с неизвестным номером вы не имеете (как вариант — подобное заявление можно послать по почте или по факсу). Существует множество способов проверить истинность этого высказывания — в самом простом случае компьютер анализирует число повторяющихся номеров, по которым звонили с обоих телефонов, в самом сложном — в архиве разыскивается оригинал контракта, где стоит чужая подпись. У операторов существует около десятка способов выяснить истину, однако процедуру, по понятным причинам, они раскрывать не стали. В любом случае на «разбор полетов» уходит до недели — после этого претензии снимают и проблемы наступают уже у дилера, который допустил такие несуразности.

В итоге следующие выводы: во-первых, купить легальные контракты сотовой связи без документов вполне возможно — заказывайте их через Интернет, где нет никакого контроля, но учтите, что его могут совершенно спокойно заблокировать. Во-вторых, если на ваше имя зарегистрировали «левые» контракты, которые вышли в «активный минус», то это не конец света — взыскивать с вас никто и ничего не будет, если выяснится, что они к вашей личности никакого отношения не имеют. Немножко нервотрепки — и все закончится написанием заявления, с которым будет разбираться оператор — бремя доказательства лежит именно на его службе финансового контроля. Виновного дилера найдут и показательно «отстрелят». В-третьих, если есть подозрения, что кто-то хамским образом использует ваши паспортные данные, позвоните в абонентскую службу родного оператора и поинтересуйтесь, сколько на вас оформлено контрактов — обычно такую информацию предоставят даже по телефону. В-четвертых, помните — этот вид «бизнеса» постепенно умирает — к примеру, адекватные prepaid платформы тарифицируют абонента в режиме реального времени без возникновения задолженности, а дилерские вознаграждения зависят от величины трафика подключенного абонента, поэтому становится все меньше охотников терять репутацию из-за лишних долларов.

Большой Брат слушает тебя

В развитии телекоммуникаций есть не только положительные моменты — благами цивилизации время от времени пользуются всякого рода террористы, экстремисты, зачастую

просто бандиты и подобные им криминальные элементы. Именно для противодействия незаконным проявлениям и была создана в свое время система оперативно-розыскных мероприятий в сотовых сетях — сокращенно СОРМ. И дело здесь совсем не в желании государства слушать «всех и вся» — такая система является мощным элементом противодействия терроризму и экстремизму в современный век информационных технологий.

Попробуем разобраться, как эта система устроена, и какой класс задач ей по силам решать. Ведь специальные документы предписывают всем предприятиям, работающим в области телекоммуникаций, включая сотовых операторов, устанавливать за свой счет на оборудование специальную аппаратуру, которая гарантирует спецслужбам полный доступ ко всем информационным ресурсам фирмы. И не только к информационным ресурсам...

Согласно приказу № 2339 от 9 августа 2000 года за подписью министра **Л.Д. Реймана**, операторам связи необходимо осуществлять приобретение и установку технических средств СОРМ на коммутационном оборудовании. По сути, все оборудование сетей телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования обязательно должно поддерживать СОРМ. Без этого легально эксплуатировать сотовые сети невозможно — ведь чтобы сдать систему связи в эксплуатацию, оператор проходит много инстанций, а по поводу СОРМа «советуется» с Госсвязьнадзором.

Поскольку оборудование для адекватного функционирования сетей поставляют в основном иностранцы, они в общих чертах, конечно, осведомлены о «российской специфи-

ке». Некоторые производители адаптируют свою аппаратуру к российским требованиям уже на заводе (например, **Rohde&Schwarz, Alcatel**), некоторые производят «апгрейд» непосредственно в России. В любом случае к любой технике тщательно присматриваются российские специалисты и с удовольствием добавляют туда свои устройства. Стоимость оборудования СОРМ для сотовых систем составляет 200–300 тыс. долларов за каждый коммутатор, а вот цена внедрения выше в несколько раз. Все подобное оборудование изготовлено целиком из отечественных компонентов и управляется программами российского производства — класс защиты информации здесь варьируется от 5 до 7.

Правда, как отметил один сотрудник спецслужб на условиях анонимности, согласно закону «проведение оперативно-розыскных мероприятий, ограничивающих конституционные права граждан на тайну телефонных переговоров и сообщений, передаваемых по сетям электросвязи, а также передача сведений об этих сообщениях допускается только на основании судебного решения». Однако, согласно нормативным документам, информация об абонентах, в отношении которых проводятся оперативно-розыскные мероприятия, а также решения, на основании которых проводятся указанные мероприятия, операторам связи не предоставляются.

Еще в 1998 году были утверждены «Технические требования к системе технических средств по обеспечению функций СОРМ», где очень подробно расписывались компоненты этой интересной системы. Состав достаточно тривиальный — специальное ПО и «железо», правда, все делилось на две части — аппаратно-программные средства в составе узла связи и такие же средства в составе удаленного пункта управления. Проще говоря, управление и получение всех

необходимых ресурсов осуществляется из территориального органа ФСБ или МВД по специальному и очень мощному ~~каналу связи, который предполагается также резервировать,~~ то есть создавать равный по мощности канал. Система полностью автономна, имеет независимое питание, напрямую связана с резервными источниками питания. Помимо всего, весь трафик шифруется — здесь активно используются новейшие разработки ФАПСИ. Кстати, у оператора весь СОРМ выглядит, скорее всего, как несколько плат и высокоскоростных каналов, через которые ФСБ и может подсоединиться.

Однако возникает резонный вопрос — для получения какой информации создавать столь глобальную и разветвленную структуру? Ответ очевиден — контроль может быть тотальным. К примеру, СОРМ знает о каждом пользователе не только его электронный, но и самый настоящий контактный адрес, а также все виды обслуживания, которые он получает (в том числе межсетевой роуминг и услуги голосовой связи). Среди прочего СОРМ обеспечивает определение телефонного номера абонента при использовании им телефонной сети общего пользования, а также электронного адреса при использовании иных телекоммуникационных сетей. При съеме статистической информации можно определить время и место сеанса связи, полностью получить доступ к его истории (логи wap-адресов в случае работы в сети Интернет, весь объем переданных данных по gprs, запись голосового трафика).

Несмотря на, казалось бы, четкие документы по СОРМ, существует и двойное толкование некоторых моментов. К примеру, в соответствии с документами, СОРМ должна иметь доступ ко всем данным о пользователе и минуя оператора — то есть напрямую. С другой стороны — представители операторов не возражают против «прослушивания эфира», од-

нако биллинг и данные об абонентах передавать не хотят, требуя решения суда.

Кроме того, существует возможность определить и местонахождение абонента во время сеанса связи. Как отмечает консультант J'son & Partners **Иван Сухоруков**, «в базовых станциях GSM-операторов стоят GPS-приемники, но, поскольку они стоят на самой БС, позиционировать они могут только точные координаты данной соты. Соответственно, отследить место положения нужного абонента можно с точностью до «радиуса соты». Другая ситуация в CDMA-подобных системах — поскольку в них абонент одновременно «ведется» несколькими базовыми станциями, то и отследить его гораздо проще (получается маленький GPS). При этом ошибка составляет в России — 10–30 м». Используя указанные данные для «наводки», вполне можно определить маршрут движения интересующего объекта и дать необходимую информацию группам наблюдения — так, впрочем, обычно и происходит. Электронные средства в данном случае — хорошее подспорье.

По техническим требованиям, СОРМ на АМТС (МЦК) должна обеспечивать одновременный контроль до 240 каналов (линий) — это совсем не значит, что десятки и сотни офицеров должны круглосуточно сидеть и слушать-слушать-слушать. Нет — есть достаточно адекватные системы перехвата, которые работают в нескольких режимах.

Есть два основных режима работы системы — полный и статический контроль. Категория «статистический контроль» означает, что разговорный канал не подключается на пульт управления, а просто в реальном масштабе времени передается информация о фазах установления соединений и данные о контролируемых вызовах.

При полном же контроле на пульт управления передается в реальном масштабе времени информация о фазах установления соединений, данные о контролируемых вызовах, а также осуществляется съем и трансляция на ПУ информации, передаваемой в разговорном тракте контролируемого абонента. У этого режима есть свои особенности. Первая и основная (самая производительная) — это фиксация разговора по ключевым словам. Среди шума и гомона эфира вычленяются ключевые фразы и, если их количество в одном разговоре переваливает определенный порог, телефоны берут на контроль. Вторая особенность — определение по голосу. К примеру, мы знаем голоса террористов, бандитов, экстремистов — компьютеру достаточно иметь в запасе 20–30 фраз для точной идентификации. Как только он «улавливает» нужный голос, автоматически идет запись и фиксация всех параметров разговора — можно регулировать настройки, и тогда результат будет более адекватным. Третья особенность — специальная, определение психотипа человека по голосу. В свое время в **Институте Биофизики** создавали замечательную систему **«Филин»**, которая достаточно четко могла работать в таком режиме — подключить ее или ее аналог к телефонным линиям — дело пары минут. А выдает она замечательные данные, начиная от краткого психологического портрета до четкого прогноза решительности, агрессивности абонента. Полученных данных даже хватает для ответа компьютера на такие вопросы, как «Способен ли он в настоящий момент применить оружие?», «Насколько он верит в то, что говорит?» и т. д. Возможно, есть и еще множество режимов работы у подобной системы — о них неизвестно, но всегда можно предполагать, что «отечественные кулибины» создают отличные и качественные продукты в этом направле-

нии. Кстати, если преступник попытается изменить свой голос, то это тоже не поможет — уже давно существуют системы, которые могут распознать даже специально зашифрованный тембр и определить не только пол, возраст, социальное положение, но и место рождения, национальность.

Теперь определимся, откуда спецслужбы берут сотовые номера, которые ставят «на карандаш». Их можно, как я полагаю, разделить на несколько категорий.

Первая — телефоны «в разработке». Это номера, полученные оперативным путем — от агентуры, опосредованно, при разборе захваченных у противника документов и т. д. Вторая — номера, на которых компьютер сосредоточил свое внимание, перехватив определенный набор внушающих опасение ключевых фраз или слов. Третий — номера, которые по различным признакам могут представлять потенциальный интерес — купленные у поставщика, перемещающегося по местам, где могут находиться базы боевиков или террористов.

Популярный сервис sms тоже «под колпаком» — ведь это, по сути своей, только набор символов, текст. А его, в отличие от голоса, можно систематизировать путем шаблонов, словарей и всевозможных комбинаций на русском и английском языках. Не очень сложно выделить на это дело небольшую часть ресурсов компьютерной системы — тем более программу перехвата, скорее всего, переделывали из взятой за основу системы перехвата пейджинговых сообщений. Еще одно удобство — текстовые послания легко хранить, ведь 160 символов совсем немного, а жесткие диски у компетентных органов огромные.

Одно дело вести контрразведку, другое — хранить государственные секреты. Здесь сотовая связь тоже помогает.

Чтобы полностью исключить возможность перехвата своих разговоров, спецслужбы в России создали специальную федеральную подсистему конфиденциальной сотовой связи (СФПКСС). В рамках федеральной подсистемы услуга **«Конфиденциальная сотовая связь»** предоставляется как для органов государственной власти, так и для коммерческих абонентов, желающих гарантированно закрыть конфиденциальную информацию. По результатам открытого конкурса **ОАО «МегаФон»** является «базовым» оператором стандарта GSM-900/1800 для этой системы. Она должна устранить межведомственную разобщенность силовых структур, таких как Минобороны, ФСБ и МВД, снабдив их абонентов единым средством защищенной радиосвязи. Планируется, что в 2004–2005 гг. эта система будет развернута в Южном, Центральном и Северо-Западном федеральных округах, а в 2005–2007 гг. — охватит всю территорию России. Первый фрагмент федеральной подсистемы конфиденциальной сотовой связи в стандарте GSM с мая 2002 г. действует в Чечне. Проект реализовали **«МегаФон»** и **ФГУП «Космическая связь»**, которое обеспечивает спутниковый канал для соединения чеченского фрагмента с основной сетью сотового оператора.

Услуга «Конфиденциальная сотовая связь» обеспечивает дополнительное шифрование речи с гарантированной стойкостью на всем протяжении соединения. **Марина Белашева**, пресс-секретарь ОАО «МегаФон»: «При использовании услуги конфиденциальной сотовой связи голосовая информация передается в закрытом виде по каналам передачи данных. Между двумя телефонами создается канал связи, гарантированно защищенный от прослушивания как в радиоэфире, так и на коммутаторе и любом другом оборудовании оператора сотовой связи». При использовании услуги «Конфи-

денциальная сотовая связь» абонент имеет оптимальную маршрутизацию трафика, а также может получить приоритетное установление соединения и возможность сопряжения с корпоративными сетями телефонной связи корпоративных пользователей.

Шифрование речи производится в специальных сотовых телефонах **«SMP-Атлас»** встроенными средствами. Специальный сотовый телефон, поддерживающий услугу конфиденциальной сотовой связи стандарта GSM 900/1800, разработан **ФГУП НТЦ «Атлас».** Телефонный аппарат сертифицирован для использования в России и за рубежом, и позволяет осуществлять гарантированно закрытую связь абонента как в домашней сети, так и при нахождении в роуминге в любой другой сети стандарта GSM, в том числе за рубежом.

Специальный сотовый телефон может работать как в открытом (96 часов в режиме ожидания, 3,5 часа в режиме разговора), так и в защищенном режиме — для переключения достаточно нажатия кнопки. В закрытом режиме телефон обеспечивает гарантированную криптографическую защиту речевой информации и аутентификацию абонентов. В открытом режиме аппарат позволяет использовать функции обычного сотового телефона стандарта GSM (речь, данные, факс, SMS). Весит он 130 грамм и стоит 2700 долларов. В Чечне этой услугой пользуются сотрудники силовых ведомств, и их единицы. Всего абонентов в Чечне около 1800 — это абоненты, находящиеся на территории ЧР (в основном юридические лица), пользующиеся услугами сотовой связи по согласованию с силовыми ведомствами (из-за ограничений на использование радиоэлектронных средств гражданского назначения) и находящиеся в закрытой группе. Закрытая группа подразумевает запрет на внутрисетевой, национальный и

международный роуминг, кроме того, в сети ЗАО «Мобиком-Кавказ» установлен запрет на предоставление услуг сотовой связи всем категориям, не входящим в закрытую группу. Стоимость одной минуты разговора соответствует тарификации в выбранном абонентом тарифном плане, абонентская плата за услугу «Конфиденциальная сотовая связь» устанавливается региональными предприятиями.

Устройство имеет несколько степеней защиты, в том числе криптографических — помимо стандартной SIM-карты сотового оператора, в телефон вставляется еще и специальная смарт-карта российской разработки. На ней записана вся информация об алгоритме шифрования, причем количество ключей шифрования составляет невообразимую величину — 10 в 77-й степени. Нажав на специальную кнопку, абонент переводит связь в зашифрованный режим. После разговора смарт-карту можно из телефона вынуть. Если враг захватит телефон, без смарт-карты он по нему позвонить не сможет. В экстремальных условиях пользоваться сотовым телефоном удобно — гораздо удобнее, чем, например, рацией. У спецтелефонов, разработанных в **НТЦ «Атлас»**, есть много интересных функций. Например, обязательная аутентификация собеседника — имя, фамилия, отчество. Или блок питания, который можно подзаряжать от аккумулятора БТР (в отсутствие бронетехники можно подзаряжаться и от обычного автомобиля).

Выводы из текста очень простые. Федеральные органы государственной власти должны преследовать на территории страны лиц, причастных к террористической де-

ятельности, независимо от того, где планировались и осуществлялись террористические акции, наносящие ущерб Российской Федерации. И государство имеет право решительно и твердо обеспечивать свою национальную безопасность законным средствами. СОРМ в этом качестве — одна из самых передовых систем.

Мобильные аксессуары

Мобильные «примочки»

Простая сотовая связь уже не устраивает большинство пользователей. Сотовый телефон перестал быть только средством связи — от него хотят гораздо большего. К примеру, скандинавы требуют от производителей сотовых телефонов оборудовать их трубки дополнительными удобствами. В телефон предлагают вставить, например, косметические зеркальца для деловых женщин. Другое предложение — пожарная сигнализация. Люди, увлекающиеся здоровым питанием, просят вмонтировать в мобильный телефон специальный щуп, с помощью которого можно определить содержание калорий в еде. Среди запросов — приборы, определяющие силу ветра, скорость подъема, давление, температуру воздуха, тела, скорость ветра, компас и многие другие. А в Италии даже спроектирован механизм для максимально быстрого попадания мобильного телефона в ладонь. Итальянский изоб-

ретатель Франко Калдана спроектировал механизм, состоящий из специальной пластинки с направляющими, по которым телефон «съезжает» в руку из рукава. Сигналом для старта является вибрация, вызванная звонком. Точно так же телефон уезжает обратно по руке вверх по окончании разговора. Вполне возможно, что скоро эти предложения будут реализованы на серийной основе — запросы рынка всегда четко отражают усилия производителей сотовых трубок.

Мало того, в Германии лицензируется устройство, которое позволит заменить звуки мобильника на запахи. Немецкий изобретатель Андреас Вульнер, которого, по всей видимости, сильно раздражали звонки мобильника, собирался запатентовать устройство, которое позволит мобильным телефонам издавать запахи вместо звуков. Пользователь сможет идентифицировать своих абонентов по запаху. Уже создан опытный образец устройства — небольшая коробочка, закрепленная на задней панели телефона. Внутри коробочки находится чип с ароматическими маслами, выбранными пользователем для разных собеседников. При каждом входящем звонке масло активизируется, и издается соответствующий аромат. Предположительная стоимость — 30$.

Для любителей экстремального отдыха теперь появился аксессуар, позволяющий не беспокоиться о батарейках для мобильных телефонов — зарядное устройство FreeCharge для мобильных телефонов, работающее на ручной подзарядке. Англо-африканская фирма Freeplay как раз представила подобный прибор, который был разработан вместе с подразделением компании Motorola, одним из крупнейших производителей мобильных телефонов. Так как разные телефоны имеют разные выходы на зарядные устройства, то Freeplay и Motorola разработали специальные насадки, позволяющие

пользоваться прибором для подзарядки телефонов от разных производителей, включая Nokia и Ericsson. FreeCharge — это средних размеров прибор, вес которого составляет 220 г, и который будет стоить порядка 70 USD. После Америки FreeCharge приедет в Европу, хотя основной пункт его назначения — развивающиеся страны. В продолжение темы можно обратить внимание тех, кто обожает выезжать на природу с сотовым телефоном, на зарядное устройство на солнечных батареях iSun от компании ICP Global Technologies. При помощи устройства можно заряжать аккумуляторы сотовых телефонов, MP3-плееров, КПК, ноутбуков и других электронных устройств. Размером не более VHS-кассеты, весом 350 грамм, устройство iSun доступно в двух исполнениях — iSun и iSunSport. Первая модель предназначена для тех, кто любит путешествовать с комфортом, вторая отличается повышенной устойчивостью к неблагоприятным погодным условиям. В комплект поставки каждой модели входит 12-вольтовый разъем подключения к прикуривателю, 7 переходников для разных типов электронных устройств. Дополнительные «примочки» для устройства будут выпущены в ближайшее время. А компания Motorola представила прототип концептуально нового аккумулятора для сотовых телефонов, который обеспечивает активную работу аппарата в течение 30 дней. Работа аккумулятора, если его можно так назвать, заключается в использовании метана. Выбор метана не случаен: во-первых, этот газ легко сжимается в жидкость, что значительно облегчает его использование. Во-вторых, его много, а добывается он из обновляемых источников. И, в-третьих, цена метана относительно невысока. Специалисты компании-разработчика утверждают, что им удалось собрать все составные части батареи в единое устройство, имеющее раз-

меры порядка 5 × 10 × 1,25 см. При работе с подобным источником мобильники смогут работать без «подзарядки» в течение 30 дней. Компания пока что не раскрывает деталей относительно того, как будет осуществляться дозаправка батарей и как скоро новые элементы поступят в серийное производство. Однако можно предположить, что первые метановые телефоны появятся в продаже через 2–3 года.

В связи со строгостями правил дорожного движения, предусматривающих штрафы для водителей которые разговаривают за рулем, на российском рынке заметно возрос интерес к комплектам громкой связи для автомобиля. Основной функцией комплектов громкой связи (Car Kits) является повышение удобства и уровня безопасности при пользовании мобильным телефоном во время управления автомобилем. Комплекты громкой связи включают в себя: держатель, устройство для подзарядки от сети автомобиля, микрофон, динамик, выход на внешнюю антенну. Некоторые комплекты также включают в себя возможность выполнения голосовых команд, устройство для уменьшения звука автомобильной магнитолы, пульт дистанционного управления, устанавливаемый вблизи рулевого колеса. По производителям комплекты громкой связи можно разделить на комплекты, выпускаемые сотовыми компаниями: Siemens, Nokia, Motorola — и комплекты, выпускаемые независимыми производителями. Изюминка рынка комплектов громкой связи — комплекты Funkwerk Dabendorf GmbH (FWD). Об уровне этого производителя говорит хотя бы тот факт, что продукцию FWD устанавливают Mercedes, BMW и Volkswagen. Система FWD Audio 2000 состоит из базового комплекта и комплекта трубки. Путем замены комплекта трубки, которая выполняется просто снятием одного держателя и установкой другого, решается

сложная техническая проблема привязки комплекта громкой связи к конкретной модели телефона.

В ближайшее время сотовые телефоны будут оборудоваться внешними источниками памяти для скачиваемого через Интернет ПО и игр, заметок органайзера — мобильные телефоны становятся по функциональности ближе к КПК (и наоборот). В этой связи актуальным становится вопрос о хранении и восстановлении данных, а факт того, что флэш-карты могут использоваться в качестве своеобразного «кэша», делает устройства более привлекательными. Компания M-Systems представила 16 Мб однокристалльный флэш-диск для мобильных телефонов, называемый Mobile DiskOnChip. По заявлению компании, новинка обладает достаточным быстродействием для использования в качестве кэша для серверных приложений. Модель отличается пониженным энергопотреблением (питание 1,8 В) и поставляется в BGA-корпусе размером 9 × 11 × 1,4 мм. В настоящее время Mobile DiskOnChip можно приобрести через дистрибьютеров в Северной Америке, Азии и Европе.

А японские KDDI и au Group выпустили на рынок «PashaPa2», новую модель цифровой камеры с флэш-памятью для подключения к мобильному телефону стандарта cdmaOne, совместимому с EZweb@mail. Устройство оборудовано ПЗС-матрицей с числом пикселей в 110.000, флэш-памятью, в которой можно хранить до 30 снимков с разрешением 120×120. Будучи присоединенной к мобильному телефону, PashaPa2 способна отображать сохраненные данные на его дисплее. С помощью камеры можно отослать фотографию по электронной почте в виде вложения в сообщение. Питание устройства осуществляется одной батареей AAA. Размеры PashaPa2 — 108 миллиметров в ширину, 32 мм в высо-

ту и толщиной в 41 мм. Производство PashaPa2 возложено на японскую компанию Kyocera.

В дополнение к новым аксессуарам стоит обратить внимание на модель, заслужившую за 2001 год всеобщее признание — это музыкальный проигрыватель Nokia HDR-1 для мобильных телефонов. С музыкальным проигрывателем Nokia потребители смогут пользоваться встроенным FM-радиоприемником и слушать загружаемые аудио/музыкальные файлы, а также использовать его в качестве портативного набора громкой связи для своего телефона. Этот стильный аппарат совместим с телефонами Nokia 3310, 3330, 8210 и 8850. «Музыкальный проигрыватель Nokia — это новое слово в эволюции аксессуаров для мобильных телефонов. Этот проигрыватель позволяет загружать музыкальные файлы формата AAC и MP3 через программу аудиоменеджера Nokia, установленную на вашем компьютере. С картой памяти емкостью 32 Мб музыкальный проигрыватель Nokia может хранить аудиоинформацию продолжительностью до часа, в зависимости от формата записи и ее качества», — заявил **Юха Рейма** (Juha Reima), Вице-президент по аксессуарам Nokia Mobile Phones.

Компания AirClic разработала новую технологию ONE-SCAN, позволяющую пользователям мобильных телефонов и других устройств с доступом в Интернет попадать на нужный web-сайт без нудного набора адреса на клавиатуре телефона или PDA. Эта система позволяет попасть непосредственно на нужную страницу, не просматривая страницу за страницей в поисках единственно нужной. Кроме того, технология предоставляет простую возможность распространения информации и совершения банковских операций при помощи уже существующих мобильных устройств. Основой технологии

является сканер штрих-кодов, разработанный Symbol Technologies, который может присоединяться к устройству или встраиваться в него. Второй составляющей является регистр CLICK-THRU, в котором хранится информация о штрих-кодах (включая EAN, UPC и JAN). В создании реестра участвовали компании, занимающиеся электронной коммерцией по всему миру. Кроме того, Symbol и AirClick совместно разработали новый штрих-код Scanlet. Применение Scanlet позволит компаниям и частным пользователям полностью контролировать и определять, на какие именно web-страницы будут отправлены конкретные клиенты. Вся эта система работает следующим образом: пользователь находит интересующий его товар в магазине или журнале, сканирует соответствующий ему штрих-код и при помощи реестра и системы перенаправления попадает на нужную страницу нужного сайта, где и находит информацию или совершает покупку. И при этом отпадает необходимость нажимать множество кнопок и тратить время на поиск. AirClick уже заручилась поддержкой таких компаний, как Ericsson и Motorola, которые заявили о возможном применении технологии в новых моделях своих телефонов.

Кроме технических новшеств, существуют и такие аксессуары, как Happy Call-держатели для сотовых телефонов. Новую коллекцию как раз представила южнокорейская компания Green Boat Co., Ltd. Необычность этих товаров для российского рынка аксессуаров заключается не только в том, что они впервые представлены на нашем рынке, но и в их функциональности. Они оповестят владельца телефона о входящем звонке песнями и плясками. Их потешный внешний вид и озорство не оставят никого равнодушными и поднимут всем окружающим настроение. Happy Call работает на час-

тотах 850–900 МГц для стандартов GSM/CDMA, а также на частоте 1,8 ГГц для указанных стандартов. Элементами питания Happy Call служат две «пальчиковые» батарейки. Этот товар имеет международные и российские сертификаты. Ожидается, что в России покупателями этой популярной за границей новинки станут владельцы мобильных телефонов со средним и выше уровнем доходов, которые ценят юмор и забавы и хотят внести элемент новизны в пользование мобильными телефонами. Кроме того, Happy Call послужит великолепным подарком для владельцев мобильных телефонов. Розничная цена Happy Call — 30–45$.

Многие пользователи сотовых телефонов хотят играть в игры по дороге на работу или, скажем, выбираясь за город на природу. В какой-то мере это позволяет сделать сотовый телефон универсальной игрушкой — уже сейчас для него существует множество игр, в которые вполне можно поиграть вдали от любимой персоналки. До последнего времени существовала одна существенная проблема — управление. В отличие от всевозможных компьютерных манипуляторов, владельцы мобильников были вынуждены ограничиваться скромными возможностями кнопочек клавиатуры. Теперь, благодаря английской компании ISMO, этой ситуации пришел конец: ею был выпущен джойстик SnakeBITE, разработанный специально для сотовых телефонов Nokia. Главное предназначение нового манипулятора — помочь играющим достичь наилучших результатов в игре Snake, набирающей все большую и большую популярность среди владельцев аппаратов Nokia. Задача этой аркадной игры — провести удава между препятствиями, одновременно поедая наивных кроликов. С каждым уровнем ваш удав удлиняется, и игра, соответственно, усложняется. Стать владельцем этого чуда

инженерной мысли можно всего за 11 USD, что, надо заметить, весьма недорого. Причем он подходит практически для всех моделей телефонов Nokia, а именно: для 3210, 5110, 5130, 5146, 6110, 6150, 7110 и ряда других. SnakeBITE крепится поверх клавиатуры и эмулирует нажатие клавиш 2, 4, 6 и 8. Несмотря на то, что джойстик разрабатывался преимущественно для игры в Snake, он вполне может использоваться и для других игр со схожим управлением. Так что любители игр на сотовых телефонах отныне смогут не чувствовать себя обделенными: специальные манипуляторы существуют теперь и для них. Однако очевидно, что это только самое начало. Ведь мобильный телефон из средства связи давно уже превратился в компактную игрушку, использующуюся всеми, кому не лень, не только для важных разговоров. Через телефон выходят в Интернет, участвуют в аукционах, играют в казино, практикуются в сочинении музыки... Неудивительно, что играют также и в компьютерные игры. И если раньше в вагоне метро можно было увидеть людей, поглощенных чтением книг, то теперь на глаза все чаще и чаще попадаются люди, активно нажимающие какие-то кнопки на своих аппаратах.

Мобильные аккумуляторы

Батарейки — сердце любого сотового телефона. Мобильность — это и автономность тоже, поэтому приходится думать о таких мелочах, как зарядные устройства, емкость аккумуляторов и потребляемые мощности. Известно, что 1 минута горения подсветки = 1 час в режиме ожидания, 10 се-

кунд работы с меню = 15 минут в режиме ожидания, 1 минута приема сетевой информации = 30 минут в режиме ожидания, одна регистрация на следующей Базовой Станции = 1 час в режиме ожидания, включение телефона с поиском и регистрацией в сети = 2 часа в режиме ожидания. А самая низкая потребляемая мощность — у телефонов цифровых стандартов (GSM 900 и 1800 МГц). И это понятно, поскольку они работают, выдавая «импульсную» мощность. Далее следует оборудование полуцифровых стандартов — таких, как D-AMPS. На последнем месте — самые энергозатратные стандарты: NMT и AMPS/NAMPS. Низкие энергетические затраты телефонов обусловлены необходимостью более плотной расстановки базовых станций. Если телефон работает на коротких дистанциях, он меньше и потребляет. Поэтому, выбирая тот или иной аккумулятор, следует помнить и об этом условии.

Кстати, для тех, кто обожает выезжать на природу с сотовым телефоном, но постоянно боится, что севшие аккумуляторы не дадут совершить важный звонок, компания ICP Global Technologies выпустила зарядное устройство на солнечных батареях, iSun.

Надо отметить, что время работы телефона от заряженного аккумулятора зависит от нескольких факторов:

1. Расстояние до соты — при плохом сигнале аппарат увеличивает мощность и, следовательно, тратит больше энергии. Это верно как для режима ожидания, так и для разговора.

2. Температура — батарея куда быстрее садится при нахождении вне разумного температурного интервала (±25°C).

3. Функции самого аппарата (подсветка клавиш, уровень звонка, вибрационный режим и т. д.) могут заметно влиять на время ожидания.

Основными параметрами аккумулятора являются:

1. Номинальная емкость — у фирменного аккумулятора этот параметр, как правило, зашифрован в его обозначении, и в обязанности продавца входит посвятить Вас в тайну этого шифра. Главное, чтобы Вы не стеснялись спросить про непонятные обозначения.

2. Реальная емкость — у нового аккумулятора составляет от 110 до 80% от номинальной емкости. Нижний предел в 80% обычно рассматривается как минимально допустимое значение для нового аккумулятора. Проверить это можно с помощью специальных устройств. Если приобретаете достаточно дорогой мобильник, то стоит обязательно проверить реальную емкость, так как в vip-моделях аккумулятор составляет значимую часть от стоимости аппарата. Попросите продавца проверить аккумулятор анализатором Cadex 7000 — получите точную информацию.

3. Внутреннее сопротивление — у новых аккумуляторов для сотовых телефонов этот показатель должен быть как можно меньше и находиться для никель-кадмиевых и никель-металлгидридных в пределах до 300 миллиОм, для литий-ионных чуть повыше. Но для всех типов аккумуляторов значение внутреннего сопротивления, приближающееся к 500 миллиОмам, говорит о старости аккумулятора или его неправильной эксплуатации. Повышенное внутреннее сопротивление аккумулятора вызывает сокращение времени работы телефона, а при очень больших значениях (более 800 — 1000 миллиОм) при входящих и исходящих звонках телефон отключается.

Чтобы не купить подделку, обязательно ознакомьтесь с сертификатом на приобретаемый товар. По российским за-

конам, аккумуляторные батареи подлежат обязательной сертификации, поэтому отсутствие соответствующего документа или отказ продавца предъявить его наводит на соответствующие размышления. Старайтесь иметь дело только с фирменными салонами. Поинтересуйтесь у продавца сроком гарантии на батарею и правилами ее эксплуатации. В приличных салонах вам обязательно дадут квалифицированный совет по использованию конкретной батареи, расскажут, как увеличить срок ее службы, и порекомендуют специальные зарядные устройства. В кратких описаниях того или иного телефона почти всегда можно увидеть характеристики аккумулятора, продаваемого вместе с телефоном, а именно — его электрохимическую систему и емкость (измеряемую в мАч). И, даже если не указано время работы телефона с данным аккумулятором, зная особенности разных конструкций оных, можно приблизительно прикинуть Talk-time и Standby (так кратко называются время работы телефона в постоянно включенном и постоянно выключенном состоянии соответственно), а также насколько хлопотно будет их обслуживание — ведь аккумуляторы чувствительны к неправильной эксплуатации. Встречающиеся сегодня на рынке батареи можно разделить в зависимости от их «наполнителя» на четыре основных вида:

1. Ni-Cd, никель-кадмиевые
2. Ni-MH, никель-металл-гидридные
3. Li-Ion, литиево-ионные
4. Li-Pol, литиево-полимерные.

NiCd — аккумуляторы с наиболее отработанной технологией, имеют более высокую энергетическую плотность и способны выдавать ток большой величины. Менее всех остальных критичны к ошибкам пользователей при эксплуатации. Допускают восстановление своей емкости, но на специальной аппаратуре и по специальному алгоритму. Самые распространенные и дешевые аккумуляторы. Сохраняют свою работоспособность практически в любых погодных условиях, выдерживают свыше тысячи циклов заряда/разряда, легко восстанавливаются при понижении емкости и после длительного хранения. Недостатки, разумеется, тоже есть: необходимость периодически полностью разряжать аккумулятор для устранения «эффекта памяти», высокий саморазряд (до 10% в течение первых 24 часов), большие габариты, относительно маленькая энергетическая плотность (отношение емкости к размеру и массе). К минусам этих аккумуляторов можно отнести и «недружественность» к окружающей среде. Сейчас они постепенно покидают рынок сотовых телефонов. В NiCd аккумуляторах рабочее вещество присутствует в виде мелких кристаллов, обеспечивая максимальную площадь соприкосновения с электролитом. При неблагоприятных условиях эксплуатации кристаллы укрупняются до размеров, в 150 раз превосходящих первоначальные, вызывая резкое уменьшение площади активной поверхности. Как следствие, снижается напряжение и уменьшается емкость. А в некоторых случаях острые грани кристаллов даже прокалывают сепаратор, вызывая высокий саморазряд или короткое замыкание. Экологически вредны при неправильной утилизации. В настоящее время новые сото-

вые телефоны никель-кадмиевыми аккумуляторами практически не комплектуются.

NiMH — разработаны для замены никель-кадмиевых аккумуляторов. При меньших размерах и массе, чем у никель-кадмиевых, обладают большей энергетической плотностью (примерно на 30% — 50%), меньшим «эффектом памяти» (некоторые фирмы-производители заявляют о полном его отсутствии). Однако по ряду параметров NiMH-аккумуляторы все же проигрывают NiCd. У них меньше циклов заряда/разряда (около 500), более высокий саморазряд (выше в 1,5–2 раза) и более высокая цена. Правда, в них меньше кристаллических сгустков, вызывающих потерю емкости — главным образом, из-за более короткого срока их службы, по сравнению с NiCd. Потерю заряда вызывает и старение. У изношенного аккумулятора пластины электродов разбухают и начинают слипаться друг с другом, что приводит к повышению тока саморазряда. Укрупнение кристаллических образований в аккумуляторах на основе никеля происходит в основном из-за слишком долгого нахождения аккумулятора в зарядном устройстве и многократного заряда без периодического полного разряда. Однако не нужно и полностью (до 1 В на элемент) разряжать аккумулятор перед каждым зарядом. Это также сокращает срок его службы. Подобную процедуру — тренировку — достаточно проводить один раз в 30–60 дней. Она позволит разукрупнить кристаллические образования. Большой диапазон емкостей. В зависимости от нее: Talk-time 2–5 ч., Standby 100–300 ч. Перед зарядом рекомендуется полный разряд. Храниться должны в разряженном состоянии. Экологически безопасны.

Li-ion — наиболее перспективные аккумуляторы для сотовых телефонов. Постепенно завоевывают позиции на рынке устройств мобильной связи. У них примерно вдвое больше емкость, чем у NiCd того же размера, низкий саморазряд (менее 1% в сутки), отсутствие каких-либо требований к обслуживанию, за исключением необходимости хранения в заряженном состоянии. Li-ion аккумуляторы повреждаются при заряде в «чужих» зарядных устройствах, а также при хранении в глубоко разряженном состоянии. Уменьшение емкости Li-ion-аккумуляторов необратимо, так как используемые в них токсичные материалы рассчитаны на работу только в течение определенного времени (к концу эксплуатации аккумулятора токсичность применяемых в них веществ снижается). Li-ion-аккумуляторы некоторых производителей могут работать только при положительных температурах, подвержены старению, даже если не используются, плюс высокая цена. Ухудшение емкости наблюдается примерно после года эксплуатации. Через два года аккумулятор практически выходит из строя. Поэтому Li-ion-аккумуляторы не рекомендуется хранить в течение длительного времени.

Li-polymer — совсем недавно появились на рынке сотовых телефонов и портативных компьютеров, они немного дешевле, чем Li-ion. Выдерживают примерно 150 циклов зарядки-разрядки, имеют высокую энергетическую плотность (больше, чем у Li-ion). Имея примерно такую же плотность энергии, что и Li-ion, Li-pol-устройства могут быть изготовлены в пластичных разнообразных геометрических формах, нетипичных для обычных аккумуляторов, в том числе достаточно тонких и способных заполнять любое свободное место.

Сравнительная таблица параметров аккумуляторов:

Параметр	Тип электрохимической системы			
	NiCd	NiMH	Li-ion	Li-pol
Плотность энергии (Втч/кг)	40–60	60–80	100	150–200
Число рабочих циклов заряда/разряда (уменьшение емкости до 80%)	1500	500	500–1000	100–150
Внутреннее сопротивление при напряжении 3.6 В (миллиОм)	100–200	150–250	150–250	Нет данных
Минимальное время заряда, часов	1.5	2–4	3–4	8–15
Устойчивость к перезаряду	Средняя	Низкая	Очень низкая	Нет данных
Саморазряд за месяц	20%	30%	10%	Нет данных
Напряжение на элемент, вольт	1.25	1.25	3.6	2.7
Ток нагрузки	>2C	(0.5–1.0) C	<1 C	0.2 C
Диапазон рабочих температур, °C	– 40...60	– 20...60	– 20...60	Нет данных
Периодичность обслуживания, дней	30	60-90	Не требуется	Не требуется

Выбор аккумулятора — дело индивидуальное. Для деловых людей интерес могут вызвать Li-ion аккумуляторы — быстрота зарядки, но высокая стоимость. Зато телефон с таким «сердцем» будет очень активным и долгое время сможет оставатся автономным. Если вы немного стеснены в средствах, однако готовы через год купить современный и лучший аккумулятор, то выбирайте NiMH. Прогресс в технологии их изготовления привел к тому, что начали появляться аккумуляторы с повышенным количеством циклов заряда/разряда (около 1000) и отсутствием требования предварительного разряда перед зарядом. Если Вы покупаете «бюджетный» телефон, то, скорее всего, столкнетесь с батареей типа NiCd. Однако стоит отметить, что аккумулятор постепенно становится неспособным принять во время заряда то количество энергии, на хранение которого он рассчитан.

Кстати, сингапурский производитель аксессуаров для мобильных телефонов, компания Emporia Telecom, выпустила специальное устройство для зарядки сотовых телефонов. Основное его предназначение — помочь тем, у кого разрядился аккумулятор в телефоне, и нет возможности его зарядить, а телефон очень нужен. Устройство, получившее название Yap, отдаленно напоминает небольшую камеру хранения. Такие устройства будут устанавливаться в общественных местах, где каждый может зарядить свой сотовый. Для того чтобы использовать устройство, необходимо набрать четырехзначный защитный код, оплатить услугу и поместить телефон в индивидуальный закрывающийся снаружи слот, соответствующий модели и габаритам телефона. После чего телефон можно спокойно оставить в «камере хранения». За сумму в 1 сингапурский доллар (около 16 рублей) устройство будет заряжать телефон 20 минут, что даст ему возможность работать приблизительно 6 часов в режиме ожидания. Всего же можно заряжать свой мобильник до 20 часов. Разблокируется закрытый слот при помощи все того же защитного кода.

О правилах обращения с аккумуляторами стоит сказать отдельно:

1. Для увеличения срока службы новые NiCd- и NiMH-аккумуляторы поставляются, как правило, в разряженном состоянии, поэтому перед использованием необходимо провести полный заряд аккумулятора. Максимальной емкости аккумулятор достигает через 3–4 цикла заряда/разряда. Это правило справедливо и для Li-ion-аккумуляторов, но они поставляются уже в заряженном состоянии и могут подзаряжаться в любом графике.

2. Для увеличения срока службы и емкости NiCd- и NiMH-аккумуляторы необходимо полностью разряжать перед последующим зарядом. Рекомендуется заряжать аккумулятор после того, как оставленный включенным телефон сам отключится из-за разряда аккумулятора.

3. Если по той или иной причине у вас нет возможности полностью разрядить NiCd- или NiMH-аккумулятор перед зарядом, сделайте это позднее. И хотя бы дважды в неделю производите циклы полного разряда/заряда.

4. Очень удобно (хотя, конечно, не всегда возможно) иметь запасной аккумулятор. Это позволит вам постоянно доводить NiCd- или NiMH-аккумулятор, находящийся в телефоне, до полного разряда и тем самым увеличить срок его эксплуатации. Кроме того, вы застрахуетесь от случайных поломок и будете избавлены от необходимости заряжать аккумулятор, если он вдруг закончит работать в середине рабочего дня.

5. Не оставляйте аккумулятор в холодных или теплых местах, например в автомобиле зимой и летом или около радиатора. Телефон с переохлажденным аккумулятором может временно не работать, даже если он полностью заряжен. Старайтесь хранить аккумулятор при температуре от 15°С до 25°С (предельные температуры для NiCd- или NiMH-аккумуляторов — от – 20°С до + 45°С и от 0°С до 45° С — для некоторых Li-ion).

6. Не стоит заряжать теплый или холодный аккумулятор. Подождите, пока он нагреется до комнатной температуры. Оптимальная температура для заряда 15-25°С.

7. Время работы с заряженным аккумулятором зависит от его реальной емкости, интенсивности разговоров по телефону, от расстояния до базовой станции, от режима работы и температуры окружающей среды.

8. Используйте зарядные устройства из комплекта поставки вашего телефона или купленные у вашего оператора сотовой связи именно для вашего типа аккумулятора.

9. Не допускайте соприкосновения и замыкания электрических контактов аккумулятора с металлическими предметами. Это огнеопасно и приведет к его повреждению. Храните аккумулятор в защитной упаковке.

10. Для надежной работы контакты аккумулятора и соответствующие контакты в телефоне должны бать чистыми и не иметь следов окисления. При необходимости удалите следы окисления ластиком и протрите спиртом.

Цветные панельки

У многих деловых людей есть сотовые телефоны, которые они постоянно носят с собой. Это — элемент престижа, уверенности в себе, подчеркивание собственной значимости. По «наворотам» и модели можно судить о толщине кошелька владельца, а по сочетанию телефона с одеждой — о наличии хорошего вкуса. Однако кроме этих показателей о многом может рассказать цвет панелей сотового телефона — это те значимые сигналы, которые каждый владелец телефона посылает окружающим. У каждого человека есть сознательная маска для окружающих и бессознательное, проявления которого мы видим в одежде, машинах, речи и, конечно цветах.

Поклонники различных оттенков красного, по утверждению психологов, больше других склонны к раздражению и вспыльчивости. В основном это холерики. Их основные про-

явления — эмоции, ясность целей, нескромность, требовательность, трудолюбие, достоинство, соперничество. Женщины: сильные личности и любят интеллектуальных мужчин, завышенные запросы, изменчивость настроения. Дети: душевное здоровье, активность, жажда любви и семейного тепла, множество желаний. Мужчины: способны заразить этой вспыльчивостью своих партнеров по разговору. Эти люди назойливы и навязчивы, стремятся подмять под себя всех встречающихся на пути. Основной их страх — страх остаться одному. Король без свиты не может быть королем, а быть простолюдинами они принципиально не могут. Если же обстоятельства сложились против них и они остались в одиночестве, лучших поклонников живописи, новомодного театра и страстных собирателей антиквариата не найти.

Те, кто оживляет свои трубки всеми оттенками зеленого, невероятно тщеславны. Люди, его предпочитающие, благодаря твердости, имеют манеру уверенно держаться. Они самоуверенны и уверенны вообще. Так как они обеспечены и уверенны в признании со стороны окружающих, то выглядят обывателями. Зеленому присущи и положительные консервативные качества: настойчивость и выдержка. Флегматики. Ощущают потребность в материнской любви. Ждут от своих собеседников постоянного подтверждения значения своей роли. Теневая сторона поведения «зеленых» — их неуверенность в себе.

Поклонники синих вставок — люди, ищущие удовлетворения, покоя и расслабления. Их основные качества — верность, дружественность, самоотдача, радость от радости, приносимой другим. Они предпочитают владеть сельским или пригородным домом, ограничиваясь в крайнем случае отделкой городской квартиры в «кантри»-стиле. Это очень

закрытые люди, не стоит рассчитывать на быстрое возникновение дружбы, общаясь с «синетрубником». При этом играют роль оттенки. Темно-синий — чаще пожилые и более образованные. Светло-синий — сверхвозбужденные, с навязчивыми идеями. Зелено-синий — гордая манера держаться. С потемнением — гордость переходит в замкнутость. Скрывают чувства. Уклоняются от общественных обязанностей, слывут оригиналами, новаторы, спекулянты. Фиолетово-синий — осознанность, прагматизм, самодовольство, но опрометчивость, честность и верность, надежность и дружественность, при склонности к уединению — общительность. Остроумие, легко берет и отдает, смена интересов.

Люди, предпочитающие желтый цвет, включая золотые оттенки, прежде всего одержимы стремлением к свободе. Их характеристика — многогранность и виртуозность, разбегающиеся мысли, разносторонность, поиски, неудовлетворенность, спекулятивность, надежды, часто фальшивые, красноречие, пылкость, дистанция. У этих людей хорошо развито воображение, и они открыты переменам. Достоинством «желтых» является их оптимизм. Они склонны к путешествиям и новым связям. Однако они не могут без публики и качеством публики не всегда озабочены.

Владельцы однотонных черных телефонов либо просто консерваторы, замкнутые, сдержанные люди, либо они повышенно агрессивны. Их позиция — «нет» в боевом протесте, конфликт, борьба с неизбежными страданиями, безверие или надежда на сверхъестественное вмешательство.

При оценке телефонов партнера стоит взвесить также такие факторы, как мода и индивидуальные особенности ситуации. Появляется масса моделей телефонных трубок, которые выполнены только в одном цвете, но при этом являются

самыми дорогими и «навороченными». Изрядная часть состоятельных граждан покупают именно такие аппараты, не обращая внимания на их цвет. Вот, к примеру, множество новых аппаратов серые, характеристика этого цвета вот такая — рутина, заурядность, заботы, грусть, печаль, беспросветность, бесперспективность, нужда, нищета. Однако это совсем не говорит так однозначно об их владельцах. Тем более гендерные различия — есть женщины, которые с удовольствием купят все предлагаемые цветные корпуса и будут менять их в зависимости от настроения, что лишит аналитика какой-либо возможности угадать основную составляющую их натуры.

Новое сердце мобильника

Если микроплаты сотовых телефонов — это «голова», то SIM-карта — это сердце сотового телефона. SIM-карта — это пластиковая карта со встроенным микропроцессором, которая является «ключом» для входа в сеть сотовой связи и несет в себе всю необходимую служебную информацию, она обеспечивает защиту от несанкционированного использования Вашего телефонного номера и позволяет создать личную телефонную книжку.

Без SIM-карты Вы можете позвонить только по телефону экстренной помощи — 112.

Прошло то время, когда SIM-карта была только хранилищем информации (20–30 SMS, записной книжки телефонов и номера абонента). В настоящее время все крупные сотовые операторы используют SIM-карты в гораздо больших объемах — они стали многофункциональными. Совсем недавно

«МегаФон» зарегистрировал миллионный запрос к SIM-меню в московской сети. «МегаФон» первым из московских операторов мобильной связи предложил абонентам новейшую услугу SIM-меню — удобное средство доставки на дисплей телефона полезной текстовой и графической информации. В отличие от других сетей, эта услуга доступна всем абонентам «МегаФона» с первого дня подключения. SIM-меню не требует дополнительной подписки и «прошито» непосредственно на SIM-карте абонента.

Пользоваться SIM-меню в сети «МегаФон» предельно просто. Последовательно нажимая две-три клавиши телефона, абонент выбирает нужный раздел в меню телефона и подтверждает запрос на информацию — практически моментально данные открываются на дисплее или поступают в виде SMS. Сегодня с помощью этой услуги абоненты «МегаФона» узнают репертуар столичных клубов и кинотеатров, устанавливают на телефон модные логотипы и любимые мелодии, получают прогноз погоды и программу ТВ, ищут номера телефонов по названию организаций, играют в Black Jack, смотрят ежедневные личные гороскопы и пользуются многими другими возможностями. Особенной популярностью пользуется раздел «Ближайшие», позволяющий получать адреса и телефоны ближайших городских объектов в зависимости от того, что ищет абонент и где он в данный момент находится. Этот сервис, основанный на технологии мобильного позиционирования, быстро находит адреса и телефоны ближайших ресторанов, клубов, автосервисов, АЗС, магазинов и различных городских организаций и позволяет сразу (через «гиперссылку») набрать номер найденного объекта (например, для заказа столика в ресторане, бронирования билетов или вызова инспектора ГИБДД при ДТП). Все або-

ненты GSMЛАЙТ могут бесплатно найти по запросу ближайшие закусочные и кафе, в которых средняя сумма счета не превышает $10. Для этого в SIM-меню необходимо выбрать рубрики: Где поесть / Fast Food / До 10 USD. Владельцы новых телефонов Nokia могут бесплатно загрузить песню Bjork «So quiet» в качестве мелодии звонка. Путь в SIM-меню: Оформление / Мелодии / Другое / So quiet. Так же просто в разделе «Оформление» можно найти и поставить на свой телефон забавную иконку, картинку или логотип, в том числе и логотип GSMЛАЙТ.

Компания «Вымпелком» не отстает от конкурента и представила на рынок новый продукт «Электронный справочник beeinfo», который позволит абонентам пользоваться широким спектром полезных услуг с помощью технологии SIM Application Toolkit. Набор дополнительных услуг, предоставляемых абонентам компании, постоянно увеличивается — их список исчисляется сегодня десятками. Чтобы воспользоваться новым сервисом, пользователям достаточно приобрести SIM-карту с электронным справочником «beeinfo». Стоимость SIM-карты с электронным справочником составляет в офисах «БиЛайн» и «Мобайл-Центр» 6 долларов, без учета НДС. Важно отметить, что существующие пользователи при замене своей SIM-карты на новую могут сохранить свой прежний телефонный номер. После покупки надо установить новую SIM-карту beeinfo в свой телефон, и множество полезной информации всегда будет под рукой. С помощью справочника beeinfo не составит труда найти ближайший ресторан, узнать репертуар кинотеатров на вечер или свой гороскоп на день, а также подключить новые и оплатить подключенные услуги связи. В марте в продажу поступил новый комплект «Би+GSM» с электронным справочником beeinfo.

Купить его, так же как и обычный комплект «Би+GSM», можно в офисах продаж «БиЛайн», а также во всех салонах сотовой связи Москвы и Подмосковья. Цена комплекта «Би+GSM с электронным справочником beeinfo в офисах продаж «БиЛайн» составит $12. В цену комплекта уже включена стартовая сумма в размере $5. Для тех, кто будет приобретать новый комплект «Би+GSM» и телефон, достаточно будет внести за сам комплект лишь стартовую сумму. «Электронный справочник «beeinfo» — это SIM-карта, которая содержит в меню записной книжки дополнительный пункт <Сервисные номера> с названиями трехзначных справочно-информационных служб, по которым можно узнать у оператора прогноз погоды, забронировать авиабилет, вызвать такси и воспользоваться массой других сервисов. В меню электронного справочника у абонента также появляется дополнительный пункт, который содержит разделы по услугам: «Информация», «Адрес», «Электронный офис» и «Платежи». Выбор этих пунктов меню активирует специальные приложения (программы) на SIM-карте, которые, в свою очередь формируют запросы для управления услугами.

А компания Мобильные ТелеСистемы предлагает новую услугу «SIM-Media», для пользования которой необходимо приобрести SIM-карту нового поколения. SIM-Media —дополнительное меню, основанное на технологии «SIM Application Toolkit». Современная SIM-Media-карта, установленная в мобильный телефон, является микрокомпьютером, который позволяет выводить текст на дисплей телефона, отправлять и получать SMS-сообщения, создавать новые пункты меню телефона, отправлять информационные запросы, т. е. обеспечивает доступ к широкому спектру спра-

вочно-информационных и развлекательных услуг. Установив SIM-Media-карту в мобильный телефон, абонент получает доступ к широкому спектру справочно-информационных и развлекательных услуг. Никаких дополнительных настроек в телефоне при этом не требуется. При замене старой SIM-карты на новую номер мобильного телефона не изменяется. Удобный интерфейс позволит в любое время и в любом месте быстро и легко получить информацию о лицевом счете абонента, узнать прогноз погоды по городам России и мира, получить горячие новости, найти информацию об интересующей организации, пообщаться с друзьями и узнать свой гороскоп, спланировать свой досуг, получить и отправить e-mail. Приобрести SIM-Media-карту или заменить старую SIM-карту можно по адресу Б. Сухаревская пл., 12. В период опытно-коммерческой эксплуатации новой услуги стоимость запроса равна стоимости исходящего SMS-сообщения согласно тарифному плану абонента. Получение информации является бесплатным. Стоимость замены карты старого образца на карту SIM-Media равна стоимости замены SIM-карты, в соответствии с тарифами на услуги абонентской службы.

Сотовые телефоны становятся сложнее, и модификация SIM-карт — прямое тому подтверждение. В скором времени нас ожидают новые технические решения от операторов мобильной связи — скорее всего, это будет расширение возможностей SMS и WAP за счет наполнения этих сервисов новым контентом.

Клавиатуры для мобильного телефона

Кто «висел» в интернет-чатах, тот знает, как затягивает подобная форма общения — жаль только, что чувствуешь себя прикованным к модему и компьютеру. Однако с течением времени это чудесное изобретение применяется и для сотовых телефонов — wap-чаты становятся реальностью, а количество ежедневно отправляемых sms во всем мире можно исчислять сотнями миллионов. Все это связано с быстротой реакции и набиванием текстовой информации — делать это с помощью стандартной клавиатуры телефона, конечно, можно, но уж больно долго, нудно и неудобно. Решение было найдено еще в 99 году — с изобретения внешней клавиатуры Chatboard. В настоящее время рынок внешних клавиатур для мобильных телефонов бурно развивается.

Набор SMS сообщений при помощи микроскопической клавиатуры сотового телефона всегда был делом хлопотным. Что уж там и говорить, если при современной миниатюризации иногда мужчинам с не самыми миниатюрными пальцами затруднительно просто набрать номер. Один из выходов — выпуск миниатюрных клавиатур специально для набора SMS сообщений, что и было сделано. С появлением специальных клавиатур для мобильников сбылась мечта пользователей — сотовый телефон дает и свободу, и мобильность одновременно.

Прогресс в развитии

Пионером стала компания Ericsson, выпустившая микроклавиатуру Chatboard (стоимость Ericsson Chatboard в диапазоне 12–30 USD). Устройство представляет собой выносную клавиатуру, совместимую со всеми телефонами Ericsson. На панели цвета «металлик» размером чуть больше визитной карточки расположена клавиатура из 49 клавиш, а также кнопки специальных функций: SMS, электронной почты, WWW приложения файлов к сообщениям и телефонной книжки. Chatboard позволяет расширить возможности телефонного аппарата для работы с текстом. Возможно оперативно редактировать записную книжку телефона, отправлять сообщения электронной почты, SMS (короткие текстовые сообщения) и даже работать в Интернете.

Компания Motorola совместно с компанией Think Outside разработали портативную клавиатуру для мобильных телефонов. Motorola iBoard совместима лишь с двумя моделями телефонов — Motorola i85s и i50sx. Оба аппарата имеют доступ в Интернет, поэтому полноценная клавиатура — это полезное добавление к таким телефонам — пользователям, например, будет удобно набирать текст для электронного или SMS сообщения. Кроме того, клавиатура iBoard имеет ряд усовершенствований. Во-первых, пользователь сможет управлять телефоном, например, открывать окна, включая программы note pad (текстовый редактор) и date book (планировщик), а также включать и выключать телефон с клавиатуры. Во-вторых, клавиатура имеет специальные кнопки для удобной навигации в Интернет, и, наконец, в-третьих, с помощью клавиатуры можно регулировать звук и активировать

спикеры. Клавиатура Motorola iBoard имеет 100% размер обычной клавиатуры для PC. С виду она очень похожа на клавиатуру Stowaway. Ну, это и не удивительно, ведь Stowaway тоже разработана компанией Think Outside (стоимость Motorola iBoard около 100 USD).

Alcatel выпускает аналог Chatboard — однако этот гаджет совместим с небольшим количеством телефонов — все модели после 511 (стоимость 35 USD). Видимо, это сделано для стимулирования к покупкам целевой группы молодежи, более других «фанатеющей» по SMS. Надо отметить, что все клавиатуры просты в подключении — надо присоединять клавиатуру к нижней части телефона и нажать, к примеру, кнопку SMS (в телефонах Ericsson). Меню телефона автоматически пролистается, и на дисплее появится окно нового сообщения, которое вы можете с комфортом набрать на клавиатуре. Затем запрос «Отправить сообщение», вы нажимаете на клавиатуре кнопку Yes — и готово! Если пользователь пожелает добавить какое-либо приложение к электронному письму — например, звуковую запись или документ, — ему нужно только нажать на клавишу приложения файлов и выбрать объект, который был им помещен на свою персональную страничку на специальном Web-сервере.

Alcatel радует своих поклонников — тем, кто доволен своим приобретением, а именно мобильным телефоном Alcatel One Touch 511, но хотел бы сделать его еще более функциональным, производитель предлагает новый аксессуар — портативная клавиатура. Новинка не просто имеет компактные размеры и привлекательный внешний вид, ее очень просто подсоединить. Она не цепляется снизу на мобильный телефон, а подключается с помощью провода. Клавиатура, которая не носит никакого названия, похоже, совместима только

с мобильным телефоном Alcatel One Touch 511 и поэтому вряд ли подойдет ко всей серии Alcatel One Touch 500. По мнению производителя, одним из самых полезных аксессуаров для мобильных телефонов является именно удобная клавиатура. Особенно это актуально для тех пользователей, которым постоянно приходится работать с текстом и обмениваться данными. Но стоит заметить, что модель клавиатуры не полноразмерная, а портативная, но в то же время за счет продуманного дизайна, с учетом эргономических показателей, а также функциональной «продвинутости», с ней очень легко работать. Клавиатура имеет несколько «горячих» клавиш, скроллинг, расположенный сбоку, и привычную раскладку QWERTY. И хотя мы больше привыкли следить за появлениями клавиатур для карманных компьютеров, но все равно подобные аксессуары для мобильных телефонов — это приятное добавление. Новинку уже можно приобрести по цене 38 евро.

Модные дополнения

Отдельная история — компания Siemens, которая на выставке CeBIT2002 представляла необычную полноразмерную клавиатуру для мобильных устройств. Для работы изображение клавиш проецируется на поверхность стола (или аналогичную ровную плоскость). После чего пользователю остается лишь нажимать на «виртуальные» кнопки. Специальный датчик считывает движения и передает информацию на устройство, к которому подключен чудо-аксессуар. Отметим, что такой манипулятор может заменить собой и мышь. Клавиатура не боится хлебных крошек и пролитого пива и может найти свое применение в мобильных телефонах, лэптопах, Pocket PC и прочих чудесах.

Производят внешние клавиатуры и сторонние фирмы — к примеру, американская компания Digit Wireless предложила пользователям модель Fastap. Дело в том, что, помимо стандартных цифровых клавиш, Fastap содержит двадцать шесть кнопок по числу букв латинского алфавита, кнопки «*» и «#», три кнопки со знаками пунктуации, а также кнопки пробела, регистра и удаления. Все эти дополнительные клавиши расположены между обычными цифровыми, а поэтому сама клавиатура остается относительно компактной. Использование Fastap позволяет в 2 раза ускорить набор текстовых сообщений по сравнению с любыми другими существующими технологиями.

Есть и уникальные предложения — английская компания Electro Textiles разработала клавиатуру из ткани, которая предназначается для пользователей мобильных телефонов и карманных компьютеров. Серийно это устройство выпускает фирма Logitech, купившая лицензию, пока только в комплектации для КПК. Ткань эта не пропускает воду, но зато проводит электронные импульсы без традиционных проводов или интегральных схем. С помощью этой клавиатуры, которая подключается к упомянутым устройствам, можно легко набрать текст для SMS-сообщений и не только для них. Но более всего в ней примечательно то, что она довольно мягкая и ее можно свернуть и положить в карман или завернуть в нее сам компьютер или мобильный телефон. Причем разработчики подчеркивают, что тканевая клавиатура очень долговечна.

Внешние клавиатуры — для тех, кто любит разговаривать пальцами. Устройства из этого модельного ряда будут увеличиваться в количествах с появлением новых моделей сотовых телефонов. Ведь внешние клавиатуры — это про-

сто спасение для тех, кого утомляет набор на клавиатуре мобильного телефонного аппарата длинных сообщений. Обычно они небольшие по размерам, относительно недороги и позволяют существенно расширить функции мобильного телефона за счет быстрого доступа к полезным функциям этого мобильного помощника.

Фантастические кнопки

Кстати, производители мобильных телефонов уже совершенствуют клавиатуры своих моделей — к примеру, новые клавиатуры созданы для моделей Nokia 7110, 3410, и для коммуникатора 9210. У модели 7110 клавиатура обладает кнопкой прослушивания речевой почты, кнопкой доступа к международной связи, быстрой блокировки и подсветкой. Модель 3410 оснащена кнопками быстрого доступа к WAP, автоматической ручной блокировки, ответом на звонок любой кнопкой звуковой индикацией нажатия клавиш. Причем и Ericsson и Motorolla и Panasonic стараются оснастить свои модели как минимум двумя новыми клавишами — быстрого доступа к wap/e-mail и к встроенному органайзеру.

Очень интересна клавиатура у Motorola T720 — здесь есть стильная навигационная клавиша-курсор которая может перемешаться по всей области экрана и служить отличным управлением для меню телефона. Клавиатура у Philips Fisio 820 при желании может быть превращена в одну большую игровую кнопку за счет удачной компоновки клавиш 2, 4-5-6 и 8. Серебристые миниатюрные клавиши у Sony Ericsson P800 отлично сочетаются с активным флипом и touchscreen, приятные звуковые щелчки дополняют звуковую индикацию нажатия. В модели Panasonic GD 67 тоже есть многофункциональная

навигационная клавиша-курсор — по возможностям чуть больше, чем у Motorolla. А в модели Siemens M50, помимо стандартных кнопок, присутствует многофункциональная X-клавиша.

Тенденции мирового рынка дополнительных устройств к сотовым телефонам показательны — как только обычные клавиатуры стали неудобны для набора SMS, то сразу появились усовершенствованные гаджеты. Теперь же новинки множатся в геометричекой прогрессии — от световых клавиатур до телефонов, которые могут печатать сообщения, распознавая речь по шевелению губ пользователя. Над этим работает японский оператор мобильной связи NTT DoCoMo. Хотя до появления коммерческого варианта читающей по губам трубки еще пройдет какое-то время, разработчики утверждают, что новое устройство положит конец громким разговорам по мобильникам и долгому набиванию sms. Владельцу телефона больше не понадобится кричать в трубку, чтобы быть услышанным, даже если вокруг стоит шум: достаточно лишь шевелить губами, а телефон преобразует эти движения в речь или текст.

Производители сотовых телефонов прислушиваются к потребностям молодых, мобильных людей, и тем тенденциям, которым они следуют. Молодое поколение воспринимает обмен сообщениями SMS как способ общения, без которого уже трудно обойтись. Спрос на услуги обмена текстовыми сообщениями наиболее быстро растет у молодежи — они растут вместе с Интернет и разговаривают. А производители в сотовых телефонах вполне успешно пытаются совмещать разговор по Интернет (Internet chat) с разговором по мобильному телефону.

Давным-давно аксессуары к мобильным телефонным аппаратам состояли из зарядных устройств и небольшого набо-

ра портативных устройств для переговоров со свободными руками (hands-free). Пора привыкать к тому, что с распространением внешних клавиатур (особенно виртуальных) будет создано новое направление рынка — аксессуар становится модным техническим приспособлением, превращающим мобильный телефонный аппарат в устройство обмена текстовыми сообщениями по SMS или электронной почте, и даже файлами в качестве приложений.

Мобильный жаргон и этикет

Аббревиатуры и «смайлики»

Одна из самых любимых функций сотового телефона — SMS. С английского эта аббревиатура переводится, как «Служба коротких сообщений» (Short Message Service), и представляет собой технологию, позволяющую посылать и принимать с помощью мобильного телефона короткие текстовые сообщения. Популярность SMS очень быстро растет во всем мире. Согласно данным, опубликованным GSM Association, во всем мире за месяц отправляется 15 млрд. SMS. С ростом популярности SMS, практически происходит смещение акцента с голосовой связи в сторону визуальной. Как принято сегодня большую часть информации передавать (получать) по электронной почте, только изредка связываясь с партнером с помощью телефона, так же и SMS-сообщения постепенно вытесняют обычные разговоры по мобильному.

Самое главное достоинство — фиксированная цена одного сообщения. В отличие от WAP-услуг, абоненту не нужно тратить времени и денег на подключение к Интернету и запросы. Пользователю очень легко оценить свои расходы. Это очень простая модель ценообразования привлекательна для студентов и людей с ограниченными бюджетами на мобильную связь. Сообщение SMS можно отправить на выключенный/находящийся вне зоны обслуживания телефон. Как только адресат выходит на связь, он его получит. Кроме этого, сообщение можно посылать абоненту, который в данный момент занят разговором, ведь сообщение идет по служебным сигнальным каналам. Популярность SMS заставила пользователей услуги приспосабливаться к быстрому и упрощенному набору сообщений. Так появились понятные только SMS-любителям фразы-сокращения. KIT — keep in touch, KOTC — kiss on the cheek, KOTL — kiss on the lips. Весной прошлого года английская компания Genie выпустила первый в мире словарь общеупотребительных сокращений для системы коротких сообщений, передаваемых на сотовый телефон, а наша статья — лишь краткий обзор этой темы.

В любой технологической революции наступает время, когда складываются определенные этические нормы, правила, законы. Так случилось с электронной почтой, когда люди стали понимать, что можно делать, а что нельзя. Например, нельзя посылать «слепую копию» письма, адресованного коллеге, своему боссу. А если пишешь незнакомцу, будь вежлив и на всякий случай поставь «смайлик». Нас никто не учил этикету на учебных семинарах, опыт и понимание пришли во время работы. Сейчас та же история повторяется с мобильными телефонами. Текстовый обмен сообщениями — одна из самых простых и распространенных форм общения

в мобильной связи. Но иногда этот сервис доставляет пользователям некоторые неудобства. Чаще всего это происходит потому, что владельцы карманных компьютеров и сотовых телефонов не учитывают особенностей общения через SMS. С просьбой ознакомить пользователей сервисом SMS с общепринятыми правилами текстового общения некоторые фирмы-производители обратились к экспертам по SMS-этикету. Прежде всего, беседа со специалистами выявила наличие территориальных отличий правил пользования SMS. Так, например, обмен текстовыми сообщениями во время совещаний в Финляндии считается вполне нормальным явлением, тогда как в США это воспринимается как проявление неуважения к собранию. Впрочем, эксперты по мобильному общению выявили и общие для пользователей SMS ошибки в разных странах, что сподвигло их сформулировать общие правила мобильной переписки для всех государств.

Во-первых, не стоит обрывать SMS-беседу без объяснения причины так же грубо, как и неожиданно положить телефонную трубку в самый разгар разговора. Стоит помнить, что SMS — это средство неформального общения. SMS не должны использоваться для официальных приглашений или информирования о важных известиях. Не стоит расстраиваться и обижаться, если вам не ответили на отправленное письмо. Сначала следует убедиться, что получатель сообщения знаком с этим сервисом и действительно получил послание.

Важно всячески подчеркивать тон текстового сообщения. Благоразумное использование символа улыбки может помочь при переписке, хотя следует помнить, что наилучший путь избежать неправильного понимания — подробнее объясняться словами. Не следует пользоваться SMS, занимаясь другими делами. Это запросто может обидеть адресата письма.

Слэнг — удел молодежи. Старшие коллеги по работе вряд ли будут в восторге от уличного жаргона.

Не стоит забывать, что координаты отправителя SMS можно легко вычислить. Анонимные сообщения лучше посылать с Интернет-сайтов. Не надо донимать SMS-беседами по ночам. В то время как одни люди поздним вечером могут бодрствовать, другие уже давным-давно спят. Если дело срочное, лучше связаться по телефону. Если до абонента невозможно дозвониться, а текстовое сообщение игнорируется, значит, этому есть веская причина. Возможно, что собеседник слишком занят, чтобы ответить. Всегда стоит помнить, что мобильный телефон в любое время можно выключить. На свете есть много вещей, которые, на самом деле, могут подождать.

Не пытайте беззащитных окружающих беседой по своему сотовому. Если люди не могут сбежать от твоих банальных разговоров (в самолете, в поезде, в автобусе, в такси или за столом), пожалей их. Не надо избирать для входящего звонка «Кукарачу», 5 симфонию Бетховена, Bee Gees или другую раздражающую музыку. Разве мало трезвона сотовых тут и там каждую секунду? Выключайте свой сотовый в театре, на концерте или в другом публичном месте.

Не надевайте на пояс более двух «гаджетов». Подобная страсть к беспроводным устройствам пока не стала большой проблемой, но с появлением многочисленных пейджеров и телефонов в стиле техно и рэйв скоро появятся пояса в стиле Бэтмена. Пресеките это в зародыше. Также не стоит звонить за рулем. Это вполне серьезно — это безумие нужно остановить. Вы не представляете, сколько на Земле людей, пострадавших от этого. Не стоит надевать headset в присутствии друзей своих. Неприлично быть на связи, одновременно ведя беседу со стоящим рядом. Никто не знает, здесь ты или там.

Не стоит впадать в зависимость от своего сотового. По известным причинам долгие сотовые разговоры вредны для здоровья. Пусть мозги шевелятся на работе. Дома — отдыхайте.

Русско-английская транслитерация

Множество сотовых телефонов могут передавать SMS, но лишь немногие могут делать это на русском языке. Подавляющее большинство — только на английском. Именно для этого придумана транслитерация — это система точной передачи букв алфавита одного языка буквами или сочетанием букв алфавита другого языка. В нашем случае транслитерация нужна для представления текста, написанного на русском языке с помощью букв латинского алфавита.

Буква	транслитерация	Буква	транслитерация
А	A	Б	B
В	V	Г	G
Д	D	Е	E
Ё	JO	Ж	ZH
З	Z	И	I
Й	J	К	K
Л	L	М	M
Н	N	О	O
П	P	Р	P
С	S	Т	T
У	U	Ф	F
Х	KH	Ц	TS
Ч	CH	Ш	SH
Щ	SCH	ь	
Ы	Y	Ь	'
Э	E	Ю	JU
Я	JA		

Смайлики

«Смайлик» (от английского smile — «улыбаться») означает, что сказанное ранее не надо воспринимать слишком серьезно. Заметьте, что чувство юмора у Вашего собеседника может быть развито гораздо хуже Вашего. Тогда самая невинная шутка без смайлика грозит превратиться в грозное оскорбление. Таким образом, смайлики выполняют важную роль в общении людей по Сети, смягчая удары и предотвращая конфликты. Используйте смайлики в письмах и сообщениях USENET, чтобы Ваши собеседники лучше понимали ваши мысли и настроение.

:-) Улыбка. Просто радость, или улыбка в ответ на шутку.

:-(Печаль: как жаль!

:-< Подавленность.

:-? Не знаю, как реагировать (например, в ответ на неудачную шутку).

:-@ Крик ужаса.

:-D Смех.

;-) Ирония: хе-хе, а вы-то думали!

:-} Ухмылка: ну-ну...

:-E Огрызнуться, показать зубы.

:-o Изумление: вот это да!

8-) Вытаращить глаза. Чаще употребляется в варианте **8-O**

:-] Сарказм (вариант — тупая улыбка).

:-[Злая усмешка.

:'-(Плач, рыдания.

%-) Смущение.

:-* Поцелуй.

:- Нерешительность.

:-# Я должен молчать.

|-) Закрыты глаза. (Вариант: китаец).

:*) Пишущий пьян.

Существует множество вариаций этих символов, но они употребляются значительно реже вышеприведенных и, чаще всего, являются фантазией употребителя. Фантазировать можно.

Жаргон пользователей сотовой связи

Компьютеры и сотовые телефоны очень сильно изменили нашу жизнь — такие слова, как *мобильность* и *свобода*, претерпели революцию. Появился и специфический жаргон — его знают не только «технари», но и самые обычные пользователи. Это часть речи социальной группы людей, которые используют в своей жизни мобильные технологии связи — она содержит большое количество свойственных только этой группе слов и выражений, в том числе искусственных, иногда условных. Множество слов из жаргона отличаются неформальным характером и являются шутливой заменой слов, которые уже существуют в нейтральной сфере литературного языка. Формальные и даже нейтральные слова рассматриваются создателями жаргона как слишком педантичные и даже высокопарные, и поэтому использование жаргона предполагает определенную свободу самовыражения в языковом поведении.

Все термины, представленные в материале, можно условно разделить на две основные группы — все, что относится непосредственно к сотовыми телефонам, как к аппаратам (аксессуары, особенности моделей и производителей), и все остальное (сервисы сотовых операторов и т. д.).

Технические особенности телефонов

Вибра — выбровызов

«Девочка» — телефон со встроенной антенной

«Мальчик» — телефон с внешней антенной

Мордашка — индикатор, дисплей телефона

Дока, манул, мануальность — документация на телефон, инструкция телефона

Кубышки — деления на индикаторе, соответствующие качеству приема сети телефоном

Мертвяк — неработающий телефон

Мобилка — сотовый телефон

Ныряльщик, утопленник — телефон, который перестал работать после того, как его уронили в воду

Обои — картина-заставка для экрана телефона

Палки — деления на индикаторе, соответствующие качеству приема сети телефоном

Парашютист — телефон, переставший работать после падения с высоты на жесткую поверхность

Перешивать, прошивка, прошива — изменять программное обеспечение телефона (ROM, EPROM, ...), менять версию ПО телефона

Распиновка — описание назначения контактов разъема телефона

Светофор — прозрачная антенна для телефона со встроенными светодиодами

Сима, Симка — SIM-карта

Слайдер — сдвигающаяся защитная крышка клавиатуры

Столбы — деления на индикаторе, соответствующие качеству приема сети телефоном

Труба — мобильный телефон

Убитый — неработающий телефон

Флип — откидная защитная крышечка клавиатуры телефона

Чатборд — аксессуар для телефона, повышающий удобство ввода символов в телефон

Шкурка — сменный корпус телефона

Аксессуары сотовых телефонов

Зарядник, зарядка — любая модель зарядного устройства для сотового телефона

Кобура — чехол с креплением на ремне для сотового телефона

Одежка (переставить одежку) — поменять сменные панели у телефона

Стакан — настольное зарядное устройство для телефона

Хэндсфри — наушник с микрофоном, подключающиеся к телефону, способному поддерживать работу с таким комплектом.

Модели телефонов

Алик — все модели телефонов от Alcatel
Банан — телефон Nokia 8110
Беня — все модели телефонов от Benefon
Бошик — телефон от Bosch
Дракоша — телефон Benefon Dragon
Женька — телефон Philips Genie
Лыжные — телефоны LG
Мотор, мотороллер, мотя — телефоны Motorola
Озя — телефоны Ozzy
Панас, порнослоник — телефоны Panasonic
Семен — телефоны Siemens
Соня, сонька — телефоны Sony
Фил, филипок — телефоны Philips
Эрик, эрэкшен — телефоны Ericsson

Сервисы сотовых провайдеров

Железная тетка — автоинформатор автоматизированной службы сервиса

Кривой номер — федеральный номер абонента, начинающийся с трехзначного кода 8902, 8903, 8910 и т. д.

Опсос — оператор сотовой связи

Мтесы — абоненты «МТС»

Пчелайн — компания «БиЛайн»,

Пчелы — абоненты «БиЛайн»,

Пчелофон — телефон, подключенный к «БиЛайн»

Трактористы — абоненты компании «Мобильные Телесистемы»

Другое

Битая трубка, кривая разлочка, отвязка — телефон после неквалифицированного снятия блокировки SIM-Lock, что вызвало нестабильную работу программного обеспечения

Беэска — базовая станция системы сотовой связи

Вапиться — пользоваться WAP-режимом

Ваять мэски — набивать sms

ГСМ, ДЖСМ — стандарт GSM

Лочить, лоченный, локинг — телефон, запрограммированный на работу исключительно с конкретным оператором сотовой связи (SIM-Lock)

Сотовик — человек, профессионально занимающийся сотовой связью

Юзать — пользоваться

Юзаный — б/у телефон

Подводя итог, необходимо отметить, что жаргон пользователей сотовой связи — это особый лингвокультурный феномен, который находится в стадии бурного развития. Жаргон отличается от ядра языка подвижностью, способностью быстро изменяться — он отражает реальное состояние дел в области распространения сотовой связи. Ему присуща высокая продуктивность, он является неиссякающим источником пополнения лексического запаса современного языка. В письменной и устной речи за ним закрепляются следующие языковые функции: первым описывать новые жизненные и технологические изменения, что позволяет эффективно обслуживать разговорный регистр для наиболее возможного по эффективности воздействия на собеседника.

Мобильный этикет

Сотовые телефоны есть уже у 25 миллионов россиян. И трели вызовов можно услышать уже не только в общественных местах или офисах, но даже в такси, автобусе, самолете (к счастью, не во время полета — жизнь всем дорога), кинотеатре и баре. Но пока разговор о «сотовом этикете» многим может показаться надуманным... До тех пор, пока чужой мобильник не начнет звенеть над ухом во время деловой встречи, в театре или кино.

Во время любой технологической революции наступает время, когда нужно сформулировать основные правила поведения в новых условиях — именно так получилось, когда появилась электронная почта, icq — и люди начали усваивать, что можно делать, а что — нельзя. Уже сейчас существует

много неприятных ситуаций, связанных с мобильной связью, которые каждый может испытать на себе, и подошло время создать некий порядок из мобильного хаоса. Всего 7 правил помогут сделать мобильную жизнь спокойнее и упорядоченнее.

Правило 1. Установите на свой телефон приятную мелодию и отрегулируйте громкость — не очень приятно несколько десятков раз за день слушать однотонный вызов, напоминающий пронзительную трель сигнала о начале атомной войны, играющий, вдобавок, с громкостью выхлопной трубы советского запорожца. Не у всех телефонов (пока!) есть полифонические мелодии, но приятный сигнал найдется у каждого. Кстати, не нужно разговаривать по «ручнику» в библиотеках, музеях, театрах и кинотеатрах, в ожидании приема у врача, а также в местах религиозного поклонения (разумеется, не только вашей конфессии) и прочих закрытых общественных помещениях, таких, например, как отделение скорой помощи. Да и в автобусах громкий эмоциональный разговор не всегда уместен. Когда в учреждении или в самолете вас просят воздержаться от использования сотовых телефонов, не делайте вид, что ничего не слышали. Нет — значит нет.

Правило 2. Не следует отвечать на телефонный звонок во время деловой встречи. Будь то собеседование, разговор с сотрудниками или подчиненными — никогда не нужно показывать, что вы недостаточно цените их время и внимание. Это раздражает собеседника и расстраивает наметившееся взаимопонимание. Вспомните, что есть голосовая почта — мобильный автоответчик, который с радостью запишет, сохранит и воспроизведет все поступившие сообщения за период, пока вы недоступны. Также не стоит брать включенный мобильник на свидание (это все равно, что назначить свидание в офисе!). Сейчас мобильник не может произвести на кого-то неизгладимого впечатления (Вы бы еще факс с собой захватили!) — сейчас это возможно, только если Вы пользуетесь одним из тех классных телефонов с космичес-

ким дизайном. В противном случае Вас, без сомнения, примут за неофита и позера. Ну, а если уж на этот же час у вас назначен важный разговор — предупредите своего партнера заранее, чтобы он не обиделся.

Правило 3. Подумайте о своей жизни — не стоит пользоваться мобильным телефоном во время вождения автомобиля без специальной гарнитуры hands free. Психологи установили, что, отвлекаясь на разговор, водитель и так представляет собой терминатора на колесах (внимание занято разговором!), а со скованными руками (одна на руле, другая держит телефон у уха) вероятность ДТП возрастает. Причем, как показывает печальная статистика, количество серьезных ДТП со смертельным исходом выше как раз у людей, занятых во время движения разговором по сотовому — не тормозят и на полном ходу вылетают на встречную полосу или врезаются в препятствия. К тому же, среди гула машин и дорожной суеты трудно принять важное решение. Легче выключить телефон или не отвечать на звонок. В крайнем случае, можно припарковаться где-нибудь и наговориться вдоволь.

Правило 4. Поменьше технократии — не стоит носить более двух мобильных устройств одновременно. Хотя это еще и не стало серьезной проблемой, большое количество разных хитроумных штучек, телефонов и пейджеров, весьма вероятно, приведет к появлению ремня, подобного тому, что использовал Бэтмен для крепления всех своих приспособлений. Также не стоит надевать наушник гарнитуры, если телефон не используется. Похоже на ситуацию, когда звонишь по обычному телефону и одновременно говоришь с кем-то, кто находится рядом: никто точно не знает, с кем из них говорят. И еще — не нужно выкладывать телефон на стол в ресторане только потому, что Вам могут позвонить. Это не Дикий Запад, и Вы — не ковбой за карточным столом в салуне с пистолетом-пулеметом наготове. Неужели нельзя быть более спокойным? Очень раздражает.

Правило 5. Групповые вызовы и совещания, организованные при помощи сотовой связи, должны быть молниеносны, как крик — разговор надо вести быстро, по-деловому точно и, по возможности, не тратя лишнего времени, даже если у вас корпоративный тариф. Помните, что есть вещи, которых окружающим слышать не обязательно — некоторые смешные истории, прибаутки, проблемы и конфликты вовсе не стоит афишировать. Неумение разобраться в обстановке может привести к печальным последствиям. Стоит ли ставить сделки и планы под угрозу без всякой необходимости?

Правило 6. Скажите звонящему, где вы находитесь, чтобы он мог предвидеть возможное отключение или отвлечение вашего внимания. А если ждете важного звонка — выбирайте тихое, спокойное место. Будет неприятно, если придется решать вопрос жизни и смерти, протискиваясь через толпу в коридоре. Тем более что в таком случае вам будет несравненно труднее показать свою деловую хватку. Также следите за тем, насколько близко в процессе разговора вы подошли к стоящему рядом — культурный владелец сотового телефона не станет во время разговора без большой необходимости подходить ближе 3–6 метров к людям, которые не горят желанием вникать в его дела. По той же причине не стоит принимать звонков в лифте — кроме прочего, связь в бетонной шахте обязательно прервется. Если подходящего места нет, то важный разговор лучше вообще не начинать — попросите перезвонить или не отвечайте на звонок, а запомните номер по определителю (можно сделать ответный звонок позже). Внимание к окружающим — признак хорошего тона. Понаблюдайте, как люди относятся к человеку, громко и не по делу говорящему по «мобильнику». Хотите оказаться на его месте?

Правило 7. Не нужно говорить по сотовому телефону громче, чем Вы говорите по обычному: у сотовых телефонов необычайно чувствительные микрофоны. Если есть эхо, обрывы связи, задержки в соединении, искажения речи, то лучше перезвонить а не над-

рываться, распугивая криком голубей. Говорите тихо и мягко, старайтесь привлекать к себе как можно меньше внимания. Времена, когда сотовый был чем-то диковинным, давно прошли, вряд ли вам удастся кого-то удивить. Некоторым людям, правда, просто не по силам говорить по телефону нормальным голосом. Возможно, они подсознательно испытывают страх, что их плохо слышат. Но это все же не повод в два и более раз повышать нагрузку на свои голосовые связки и, соответственно, чужие уши.

Итак, правила известны. Кому-то они покажутся простыми. Кому-то невыполнимыми. Наверное, мы все-таки освоим их — рано или поздно.

Ведь большая часть этих заповедей не вступает в противоречие со здравым смыслом.

Содержание

Мобильные аксессуары

Мобильный жаргон и этикет

Научно-популярное издание

Серия книг «Мой мобильный телефон»

Букин Максим Сергеевич

Всё про Ваш мобильный телефон

Книга 3

Редактор — А.И. Осипенко
Корректор — И.Д. Королёва
Компьютерная вёрстка — А.С. Варакин
Обложка — М.К. Выборнов

Изд. лиц. ИД № 01844 от 22.05.2000 г.
Подписано в печать 29.05.04 г.
Формат 84X108/32. Бумага для печати «Авеста». Печать офсетная.
Усл. печ. л. 6,5. Заказ 74

Издатель Осипенко Александр Иванович / «МАЙОР»
111395, Москва, Молдагуловой, 16-2-215, тел. (095) 373-04-20.
E-mail: majorpub@mtu-net.ru; http://www.majorpub.ru.