Пособие по взлому и защите телефонных сетей

Как ломают телефонные сети

ВНИМАНИЕ! АВТОР ЭТОЙ КНИГИ ПРЕСЛЕДУЕТ ЕДИНСТВЕННУЮ ЦЕЛЬ — НАРОДНОЕ ОБРАЗОВАНИЕ! ПОЭТОМУ ИСПОЛЬЗУЙТЕ ИНФОРМАЦИЮ, КОТОРАЯ СОДЕРЖИТСЯ В ЭТОЙ КНИГЕ ТОЛЬКО ДЛЯ КОНСТРУКТИВНЫХ И МИРНЫХ ЦЕЛЕЙ.

Материал этой книги поможет Вам также вести борьбу с компьютерными преступлениями.

Москва

Литературное агентство «Бук-Пресс»
2006

УДК 004.5
ББК 32.973.26-018.2
Л47

Леонтьев Б. К.

Л47 Как ломают телефонные сети. Пособие по взлому и защите телефонных сетей / Борис Леонтьев, 2006. - 320 с.

Такого вы не встретите больше нигде! Только в этой книге вы найдёте полное собрание невероятно эффективных и реальных методов взлома и защиты телефонных сетей! Невозможно перечислить здесь имена всех авторов, у которых мне довелось учиться и материалами которых я пользовался, хотя многие из них упомянуты в конце книги. Я особенно обязан Ивану Фролову, познакомившему меня с фрикингом, а также Дмитрию Яценко, который побудил меня заняться IP-телефонией, хотя они могут и не согласиться с мнением, изложенным на страницах этой книги. Я также хочу поблагодарить своего друга Максима Райкова за то, что он прочел эту работу в рукописи и высказал много ценных замечаний, и Ирину Царик за постоянную поддержку и усердный труд по подготовке книги к публикации.

Издание, как и книга Бориса Леонтьева «Фрикинг не для дилетантов», предназначено для пользователей персонального компьютера, которые интересуются проблемами взлома и защиты телефонных линий, и желают получить исчерпывающие сведения о способах несанкционированного получения информации.

УДК 004.5
ББК 32.973.26-018.2

Введение

Развитие средств коммуникаций, радио и телевидения

Для передачи какой-либо информации (звук, изображение, текст) по сети электрической связи необходимо сначала превратить информацию в электрические сигналы, затем направить ее через линии связи, а при приеме преобразовать полученные сигналы в исходную информацию. Такого рода преобразование происходит в аппаратах связи — телефонном, телеграфном, приемном и передающем (оконечных) устройствах радио и телевидения.

Впервые идею передачи текстовой (буквенной) информации на расстояние реализовал французский инженер К. Шапп. В 1791 г. он построил первый семафорный аппарат, просуществовавший до 1852 г. Связь осуществлялась визуальным образом: взаимное расположение стрелок (отвечавшее принятой системе условных обозначений) на башнях, построенных на возвышенностях, наблюдали с других башен в подзорные трубы. Число семафорных станции Франции к середине XIX в. достигло 556.

В 1830-х гг. российские ученые-изобретатели П.Л. Шиллинг и Б.С. Якоби разработали основы телеграфной связи.

В 1832 г. П.Л. Шиллинг изобрел первый телеграфный аппарат.

В 1837 г. американский изобретатель С. Морзе разработал телеграфный аппарат, который использовал кодовое обозначение каждой буквы алфавита с помощью комбинаций длинного и короткого сигнала (точки и тире) — азбуки Морзе.

В 1843 г. начала действовать первая междугородная (Санкт-Петербург — Царское Село) телеграфная линия на аппаратах Б.С. Якоби.

В 1844 г. появилась телеграфная связь между Вашингтоном и Балтимором на аппаратах С. Морзе.

В 1854 г. французский механик Ш. Бурсель высказал предложение об использовании электрического тока для передачи звуковых сигналов. Через несколько лет эту идею реализовал для передачи музыкальных сигналов немецкий изобретатель Ф. Рейс («музыкальный телефон»).

В 1855 г. английский изобретатель Д.-Э. Юз построил первый применимый на практике буквопечатающий телеграфный аппарат для передачи со скоростью 40 слов в минуту. В том же году итальянский физик Дж. Казелли предложил конструкцию фототелеграфа для передачи на расстояние изображений, основанный на электрохимической записи при приеме.

В 1864 г. шотландский физик Дж.-К. Максвелл создал теорию электромагнитных волн.

В 1866 г. закончилась прокладка первого трансатлантического телеграфного кабеля, соединившего Европу и Америку.

В 1870-х гг. французский инженер-механик Ж. Бодо изобрел телеграфные аппараты, которые позволяли по одному и тому же кабелю передавать одновременно несколько сообщений.

В 1876 г. американский инженер-электрик А.-Г. Белл изобрел телефон — аппарат, преобразующий звуковую информацию (голос) в колебания электрического тока, с последующей передачей их по линии связи и обратным преобразованием в звуки. Оконечные аппараты телефонного устройства — это микрофон и собственно телефон.

В 1877 г. венгерский инженер Т. Пушкаш разработал проект первой телефонной станции, который был затем реализован в США (Нью-Гавана). В том же году телефонная связь впервые была использована в военных целях (война Болгарии против Турции). Была сооружена 16-километровая телефонная линия между Ставкой действующей армии и г. Порадимой, где располагался штаб императора Александра II.

В 1878 г. русский физик П.М. Голубицкий сконструировал телефонный аппарат с кольцеобразным магнитом — прообраз современных телефонных аппаратов.

В 1879 г. появились первые европейские телефонные станции (Париж), а в 1881 г. — одновременно в Москве, Петербурге, Одессе, Варшаве и Ревеле (Таллине).

В 1881 г. появились первые телефонные справочники (в Берлине и Нью-Йорке), а также первые телефоны-автоматы.

В 1885 г. русский инженер П.М. Голубицкий разработал проект автономной телефонной станции с электропитанием от центральной батареи, расположенной в самой станции.

В 1888 г. немецкий физик Г. Герц смог получить радиоволны и исследовать их свойства.

В 1889 г. американский изобретатель А.-Б. Строунджер разработал проект АТС — автоматической телефонной станции того типа, какой используется до сих пор.

В 1895 г. русский инженер А.С. Попов и одновременно с ним итальянский изобретатель Г. Маркони сконструировали первые радиоприемники. Первые радиосообщения передавались в виде коротких и длинных сигналов с помощью телеграфного ключа, применением системы кодового обозначения букв алфавита — азбуки Морзе.

В 1897 г. изобретатель из Страсбурга К.-Ф. Браун сконструировал первую электронно-лучевую трубку.

В 1898 г. в России была построена рекордная по тем временам (660 км) воздушная (провода на столбах) телефонная линия (Москва — Санкт-Петербург).

В 1899 г. в России была построена линия беспроводной (радио) связи длиной 40 км. Зимой 1899—1900 гг. благодаря радиограмме, переданной по этой линии, ледокол «Ермак» спас рыбаков, унесенных штормом в море. Она была также успешно применена при спасении броненосца «Генерал-адмирал Апраксин», потерпевшего аварию у острова Гогланд на Балтике.

В 1901 г. Г. Маркони провел первую радиопередачу через Атлантику.

В 1907 г. петербургский ученый Б.Л. Розинг получил патент на «способ электрической передачи изображений». К 1912 г. Розинг разработал основные элементы черно-белого телевидения, включая систему развертки на 12 строк (в современных системах — 800 строк).

В 1923 г. американский ученый русского происхождения В. К. Зворыкин изобрел иконоскоп — передающую электронную телевизионную трубку (более совершенную по конструкции, чем у Бэрда). Телевизионная трубка (кинескоп) Зворыкина стала основным элементом современных телевизоров.

В 1926 г. шотландец Дж.-Л. Бэрд впервые публично продемонстрировал телевидение.

В 1940-х гг. начались регулярные телепередачи (США, СССР).

В 1956 г. американская фирма «Ампекс» выпустила первую видеопленку.

В 1960 г. японская фирма «Сони» выпустила первую партию транзисторных телевизоров.

В 1969 г. японская фирма «Сони» выпустила первый видеомагнитофон.

В 1982 г. в Японии (фирмы «Хитачи» и «Сони») начался выпуск телевизоров с повышенной четкостью изображения, которую обеспечивал 1125-строчный экран.

В 1980-х гг. фирмой «Мицубиси» создан полиэкран размером 6х9 м, работу которого обеспечивали 25 тыс. электронно-лучевых трубок.

В 1986 г. началось широкое использование волоконно-оптических световодных кабелей для прокладки высокоэффективных телефонных линий.

В 1990 г. голландская фирма «Филипс» наладила сборку трех моделей цветных телевизоров на жидких кристаллах с рекордным размером экрана: 3х4 м, 4х5,5 м, 6х8 м, толщиной всего 0,7 м, предназначенных для демонстрации изображения в общественных местах.

В 1990-х гг. появились и сразу широко распространились спутниковые радиотелефоны, работу которых обеспечивают космические аппараты — телефонные спутники со стационарными орбитами, а также аппараты сотовой связи, работу которых обеспечивает система наземных приемопередающих станций.

Рождение фрикинга

Фрикинг — несанкционированное получение информации (в т.ч. шпионаж) при помощи электронных устройств, а также путем несанкционированного подключения к телекоммуникационным сетям.

Фрикер — это не тот кто «взламывает» таксофонный аппарат (просто хулиган), это специалист в области электроники применяющий свои знания в промышленном (экономическом) шпионаже или извлекающий выгоду путем «электронного» мошенничества.

В 1954 г. корпорация «Bell Telephone System» (в простонародье — «Ма Bell»), в то время — крупнейший монополист в сфере обеспечения телефонных услуг, перешла на новый стандарт телефонной сети. Это решение обошлось компании в миллиарды долларов, но сделало управление мировыми коммуникациями более удобным и гибким. Замысел заключался в том, чтобы все операции производились посредством мультичастотных сигналов. Для каждого действия, будь то соединение с абонентом или переключение на междугороднюю связь, телефон отправлял на АТС сигнал определенной тональности. В 50-е годы для «Ма

Bell» это была оптимальная система. В середине 70-х она превратилась для компании в ночной кошмар.

Джои «Whistler»

Джои Энгрессиа было 8 лет, когда он впервые заинтересовался телефонами. Мальчик с рождения был слеп и большую часть времени проводил дома. Поэтому именно телефон, дававший возможность общаться со всем миром, стал его лучшим другом. В раннем возрасте у Джои обнаружился абсолютный слух. Он любил часами слушать щелчки и звуки, исходящие из трубки, стараясь затем воспроизвести их самому. Однажды, во время очередного звонка, Джои просвистел один из выученных сигналов и соединение тут же прервалось. Он позвонил оператору «Bell» и поинтересовался, почему его свист разорвал связь. Работник компании попытался объяснить ребенку строение телефонных сетей — тогда Джои не совсем его понял. Но с годами, в течение которых Джои Энгрессиа научился издавать губами свист любой тональности, он узнал о таких тайнах «Ma Bell», в которые не были посвящены многие сотрудники корпорации. И которые позволяли ему играть телефонными станциями словно марионеткой.

В 1968 г. 19-летнего Джои во время нелегального бесплатного разговора с приятелем по межгороду поймали. Это был небывалый случай и в прессе юного телефонного жулика представили чуть ли не восьмым чудом света. Но, возможно благодаря своей врожденной болезни, парень отделался лишь предупреждением. Сразу после статьи о «подростке, умевшем звонить по межгороду бесплатно», Джои стал ежедневно получать множество звонков из всех уголков Америки. Ему звонили молодые ребята, большинство из которых также были слепы, которые, как и он, фанатично интересовались телефонными сетями и могли проделывать с ними невероятные вещи. Никто из них до публикации материала в газете не был знаком друг с другом, никто даже не подозревал, что на свете есть единомышленники, так же исследующие недра корпорации «Ma Bell». Кто знает, как бы повернулась история, если бы сотрудники телефонной компании не поймали тогда Джои, если бы журналисты не рассказали об одаренном американце. Но факт остается фактом — эта статья объединила любителей телефонных сетей. И именно она проложила дорогу новой субкультуре, которая позже получила название ФРИКИНГ.

Сообщество телефонных фрикеров

В 1971 г. «Ma Bell» опубликовала в техническом журнале «Institution of Post Office» полный список частот, используемых для управления телефонной системой, а также их описания и производимые действия.

Год спустя этот список появился в «Sunday Times». Непонятно, зачем компания это сделала, но столь ценная информация попала в руки уже сформировавшегося движения телефонных фрикеров, что помогло им значительно поднять уровень своего мастерства. Фрикерами (phreaking = phone + freak + hacking) называли преимущественно молодых ребят, которые отлично разбирались в телефонных сетях и умели пользоваться их скрытыми возможностями. БОльшая часть фрикеров делилась на два лагеря: тех, кто презирал корпорацию-монополиста и своими поступками боролся против ее власти, и тех, кто мечтал работать в рядах операторов «Ma Bell». В том же 1971 году сообщество фрикеров узнало, что подарочный свисток, вкладываемый в каждую коробку с быстрым завтраком «Капитан Кранч», производит свист частотой 2600 Гц. Именно эта частота использовалась телефонной компанией для предоставления междугородних услуг. Достаточно было просвистеть в трубку и не платить за переговоры ни цента. Сейчас многие источники утверждают, что обнаружил свисток Джон Дрэйпер, впоследствии позаимствовавший у коробки название для своего псевдонима. Но на самом деле это было открытие компании слепых подростков, среди которых был Джои. Благодаря Джону о свистке узнали другие фрикеры.

Чтобы облегчить издевательства над телефонными сетями, фрикеры пользовались устройствами, под названием «Multi Frequency box» (потом они переименуются в «blue box»). Это были небольшие коробочки с кнопками и динамиком, позволявшие генерировать сигналы разных тональностей. Прародителем blue box'а был студент Массачусетского Технологического института Стюард Нельсон, который в 1964 г. написал на компьютере TX программу, генерировавшую сигналы различных частот. С ее помощью Стюард мог звонить в любую точку мира, не думая об оплате. Самые простые blue box'ы служили для бесплатных междугородних переговоров, более сложные имели широкий диапазон действий. Некоторые фрикеры мастерили заветные изделия пачками и продавали заинтересованным людям (которых было предостаточно) по цене 300$, а супернавороченные девайсы обходились покупателям в полторы тысячи. Фрикеры не ограничивались халявными звонками, они могли создавать телефонные конференции, прорывать сигнал «занято» и прослушивать разговоры, сбрасывать собеседника с линии, переключаться с одного узла на другой, заставляя свой звонок проходить через весь мир. А самые опытные были в состоянии полностью установить контроль над городской АТС и манипулироваться телефонными номерами. В начале 70-х гг. среди фрикеров была очень популярна телефонная конференция «2111», на которой они делились новыми трюками, обсуждали старые баги «Ma Bell» и рассказывали друг другу о шутках, которые проворачивались по телефону.

TAP — первый фрикерский журнал

В 1971 г. в журнале «Esquire» была опубликована большая статья Рона Розенбаума «Secrets of the Little Blue Box», в которой автор рассказал о сообществе фрикеров, самых известных представителях этого движения, об уязвимостях телефонной компании и строении blue box. История Рона произвела огромное впечатление на многих подростков, впоследствии ставших серьезно заниматься исследованием сетей «Ma Bell». В 1973 г. начинает выходить специализированное фрикерско-анархистское издание под названием «Technological Assistance Program», редактором которого был известный телефонный взломщик Al Bell. Материалы, печатавшиеся в TAP, в основном были конфиденциальными техническими документациями телефонной корпорации, разбавляемые фрикерскими трюками, инструкциями по изготовлению взрывчаток/отмычек и полезными советами о том, как пользоваться благами цивилизации бесплатно. Издание было своего рода учебником, библией для начинающих телефонных хулиганов и будущих операторов. В 1975 г. на невзрачную газетку, выходившую на четырех полосах, подписалось 30 тысяч человек. В 1983 г. TAP уже был готов к тому, чтобы ознаменовать слияние фрикинга и хакинга, но неожиданный пожар, охвативший дом Тома Эдисона (в конце 70-х он стал новым редактором) разрушил все планы коллектива. Позже стало известно, что это были одновременно и поджог и ограбление — из дома Эдисона похитили компьютер, все дискеты, имеющие отношение к TAP и записи. Авторы издания впоследствии упорно твердили, что поджигателей наняла телефонная компания, но доказательств этого не было. Оправиться от удара газета не смогла и через несколько месяцев в свет вышел последний номер.

Фрикеры в действии

В начале 80-х гг. с появлением первых персональных компьютеров, фрикинг был еще достаточно популярным увлечением, но уже начинал уступать место компьютерному взлому. Многие фрикеры, развлекавшиеся с телефонными сетями в 70-х гг. несколько лет спустя стали элитой хакерского андеграунда: Lex Luthor, Cheshire Catalyst, Nightstalker, Dave Starr, Кевин Митник и Кевин Поулсен. Впрочем, основы фрикинга знал каждый хакер 80-х.

С мучительно медленной скоростью модемов и постоянными звонками на ББС, находящиеся в других штатах, бесплатный межгород был критичен. К тому же, старушка «Bell» настолько кишела багами, что грех было не воспользоваться этим ее достоинством. На фоне громких компьютерных взломов, обильно освещаемых СМИ, фрикинг в 80-е и 90-е годы прожил тихую и незаметную жизнь. Если не считать нескольких исключений.

В 1981 г. Иан Мерфи, более известный как Captain Zap (Pat Riddle), со своего домашнего компьютера проник в компьютерную сеть телефонной компании AT&T и изменил систему подсчета тарифов за телефонные переговоры. В течение двух дней десятки тысяч людей, звонившие днем, разговаривали по цене ночного звонка. Соответственно те, кто разговаривал по межгороду ночью — платили втрое дороже.

Федеральная Коммуникационная Комиссия в августе 1989 г. закрыла Чикагскую радиостанцию WLUP-FM, предварительно оштрафовав ее владельцев на круглую сумму. А все из за популярного шоу, ведущие которого — Джонатан Брэндмейер и Кевин Мэттьюз — проводили в эфире грязные телефонные шуточки и любовались реакцией людей. Они звонили с угрозами и фальшивыми предложениями многим знаменитостям (скрытые телефоны которых получали благодаря своим фрикерским навыкам), публично разводили простых людей. Это было бы похоже на розыгрыши, если бы все выдуманные ими шутки не приносили людям неудобства. А иногда — сердечные приступы.

В 1993 г. в Лос Анджелесе три радиостанции провели конкурс, условием которого было дозвониться ровно 102 по счету. Призы разыгрывались не маленькие: 2 путевки на Гаваи, 20 тысяч долларов и автомобиль «Порше». Блокировать эфирные телефоны таким образом, чтобы в определенный момент на радио могли дозвониться только они, для опытного фрикера и хакера Кевина Поулсена с двумя его приятелями было не труднее, чем открыть банку пива. В результате троица выиграла все призы, не оставив ни единого шанса «конкурентам».

На протяжение 90-х гг. настоящей головной болью для телефонных операторов была легендарная фрикерская группа «The Phone Masters». Она долгое время нелегально пользовалась услугами «Sprint Long Distance», удаленно управляла юго-западным подразделением «Ma Bell», хозяйничала в компьютерной сети «GTE». Они могли получить доступ к самым секретным телефонным номерам (например к внутреннему телефону президента США), устанавливали прослушивание за правительственными организациями, водили за нос телефонных экспертов и могли вытворять с телефонными сетями все что угодно. Выследить троих членов группы заняло у ФБР много времени и сил, но в 1995 г. «телефонные мастера» были арестованы.

Как известно в Лас Вегасе запрещена проституция. Но спрос есть... есть и подпольное предложение. Многие предприниматели нанимали девочек и создали услуги «заказа по телефону эротического танца на дом». До недавнего времени в «городе, который не спит» было достаточно много контор, делающих такие предложения. Телефоны в них раскалялись добела — заказы поступали всю ночь, не переставая. Но внезап-

но все звонки прекратились. Из обычных ста звонков за ночь их количество упало до нуля. Обанкротившимся хозяевам контор ничего не оставалось, кроме как закрыть свои лавочки. Одна за другой они исчезали, но в то же время росла империя мосье Сорано «Vegas Girls». В прошлом — одна из тех самых контор, в которой во время кризиса количество звонков мистическим образом не снизилось, а наоборот, значительно возросло.

В компьютерном андеграунде ходили слухи о причастности к этому делу опытного фрикера, которого Сорано нанял для устранения конкурентов. Но доказательств этого не найдено до сих пор.

В 1969 г. впервые был запущен проект «ARPANET». А ровно через 9 лет мир узнал, что такое Bulletin Board System. Так, в конце 70-х гг. началась великая эпоха BBS.

Фрикинг и его последствия

История эта произошла не так давно в одном из провинциальных городов России. Двое подростков 16 лет, один из которых уже длительное время интересовался разными хакерскими делами, а другой просто за компанию, решили углубиться в область телефонии. Назовем их Коля и Андрей. Начать решили с самого простого: телефонная трубка, дисконабиратель, крокодильчики. Главная идея акции заключалась в том, чтобы подсоединиться в распределительном щитке к телефону одного человека и попытаться позвонить по межгороду. Следует заметить, что жертва была выбрана далеко не наобум, путем «оперативно-розыскных» мероприятий было выяснено, что у данного человека абсолютно халявный выход на межгород, и что он в отпуске. То есть никто бы не пострадал ни морально, ни материально. Одним ранним утром ребята вышли «на дело». Только с помощью зажигалки начали зачищать проводки, как тут неожиданно услышали скрип тормозов возле дома. Сработал инстинкт самосохранения, «фрикеры» едва успели отбежать от злополучного щитка и спуститься на площадку между этажами. Распахнулись двери лифта и оттуда вывалилась «зондер-команда» милиции в полной экипировке, немного потолкавшись у дверей квартиры, они начали спускаться по лестнице и наткнулись на нервно курящих ребят. Спросив, для порядка, что подростки тут делают и не замечали ли они ничего необычного, милиция загрузилась в свой УАЗик и благополучно уехала.

Тут бы незадачливым «фрикерам» сообразить, что «это ж-ж-ж неспроста» и отложить свою операцию до более лучших времен. Но стабильно охлаждаемый алкоголем всю предыдущую неделю мозг начал давать сбои и они полезли к щитку снова. На этот раз милиция подобралась

незаметно — ребята едва успели спрятать «фрикерский» девайс в рюкзак. Менты для начала вывернули у них карманы, и, конечно, ничего не обнаружив, нехило растерялись и уже было отпустили. Но тут одного мента, видимо более образованного, чем остальные (на одну школьную четверть), совершенно не кстати озарило: «А что это у вас в рюкзаке?». И, обнаружив трубку с крокодильчиками, менты радостно погрузили «фрикеров» в машину и отвезли в участок. Дальнейшее больше напоминало кадры из фильма «Ненависть» или обращение с пойманными партизанами в Гестапо... По приезду в отделение милиции, выбежал мордастый мужик (следователь) и начал со всей силы бить «трофейной» телефонной трубкой по голове Андрея. Потом пришел второй следователь и повел Колю с собой, тот еще было обрадовался, что не попал к психу, который в это время избивал Андрея. Но, как оказалось, обрадовался рано. В своем кабинете следователь посадил его на стул, и начал со всей силой здорового мужика методично избивать щуплого подростка, нанося удары по голове. Коля несколько раз терял сознание и уже не надеялся выйти живым из застенков милиции. Затем побои внезапно прекратились и, записав анкетные данные, следователь начал зачитывать какие-то совершенно левые статьи из УК — мошенничество, и т.п. Еще больше запутав Колю, он повел странную беседу, постоянно пытаясь вывести подростка на признание в том, что они с Андреем грабили квартиры. Причем все объяснения Коли о реальном положении дел следователь просто игнорировал. Тут только до Коли дошло, почему так оперативно приезжала милиция: Квартира, к телефону которой они пытались подключиться, была «на охране», а система охраны была связана с отделением милиции по телефону!!!

Не добившись так нужного ему признания, следователь сменил тактику и начал предлагать сомнительного рода сделки: давай ты мне все рассказываешь о своих друзьях (с упором на ограбления квартир), а я ничего не говорю твоим родителям, не порчу тебе жизнь по месту учебы и т.п. шняга. Коля упорно отвечал, что рассказывать ему (а уж в особенности про квартирные кражи) нечего. Допрос явно зашел в тупик. Сняв отпечатки пальцев, Колю отпустили. Как оказалось позже, Андрей также отделался исключительно моральным и физическим ущербом, но никак не уголовным делом. Зачем я вам рассказал эту, на первый взгляд обычную, историю? В журнале Хакер очень много пишут о том, как делать различные не совсем законные и зачастую небезобидные вещи, но почему-то я не встречал статей о последствиях таких действий. Я никоим образом не призываю вас отказаться от захватывающего мира хакинга, просто будьте внимательней и почаще задумывайтесь о безопасности самого дорогого, что у вас есть — вашей задницы.

Фрикеры, хакеры, МГТС... Отключайся!

В Мосгордуме прошли слушания по телефонному пиратству, инициированные председателем комиссии по законности и безопасности МГД Олегом Бочаровым.

О том, насколько глобальна проблема несанкционированного проникновения в телефонные сети столицы, можно было судить по количеству прессы и числу приглашенных участников. Кроме депутатов, на слушания собрались 18 представителей организаций, которые в той или иной мере должны защищать горожан от нападок фрикеров.

От пострадавшей стороны прибыли чины из МГТС и «Ростелекома». Интересы москвичей представляли депутаты, среди которых также оказались жертвы телефонного беспредела. На 700 целковых пираты «наказали» депутата Васильева.

Завесу тайны о масштабах деятельности фрикеров и баснословных доходах, сравнимых с прибылями от нелегальной торговли оружием, наркотиками или краденым автотранспортом, слегка приоткрыли сотрудники управления «Р» при МВД РФ и ГУВД столицы. По словам начальника московского управления «Р» Дмитрия Ченчугова, рентабельность незаконного переговорного пункта превышает десятки тысяч процентов. И этот вид преступности — лишь малая часть айсберга злодеяний в сфере высоких технологий. Правоохранители коснулись только непосредственной темы слушаний, обойдя вниманием Интернет-перехватчиков, ворующих чужое время пребывания в «паутине», подделку кредитных карт и хищения из виртуальных магазинов.

Логика слуг закона понятна — боялись испугать. А надо было. Законодательные дыры, куда почему-то утекают наши деньги, огромны. Приведенная блюстителями порядка аналогия с оружием более чем уместна. За его незаконное хранение уже положен срок. Здесь же оперативники вынуждены дожидаться факта телефонного «убийства» и только после него начинать розыскные и следственные мероприятия. Сейчас фрикеров, большинство из которых выходцы из Азии и Африки, задерживают за нарушения правил регистрации в Москве, а дело возбуждают по 165-й статье УК РФ — «Причинение имущественного ущерба путем обмана или злоупотребления доверием». При благополучном раскладе максимальный срок — пятилетка.

МГТС, оправдываясь, приводит свои доводы. По самым скромным подсчетам, на оборудование, гарантирующее защиту от незаконного подключения, необходимо 12 миллионов долларов. Меж тем только за последние полтора года сменилось четыре поколения устройств подмены абонентского номера. Причем себестоимость коробочки, перехватывающей и запоминающей чужой номер, составляет всего 50 «зеленых». Отечественные «кулибины» своей изобретательностью убивают у телефонистов всякое желание бороться с фрикерами, и те, не мудрствуя лукаво, спихивают свои денежные потери на горожан.

В законе о защите прав потребителей ясно сказано, что потребитель имеет право на безопасность услуги, а затраты на ее обеспечение целиком лежат на том, кто ее предоставляет. Живи мы в Америке, МГТС давно бы разорила первая пятерка пострадавших от телефонных «кидал». Там операторы связи с широко открытыми глазами идут на такие убытки. Но мы не в Америке.

Как заявил представитель МГТС, сейчас компания не отключает обманутых фрикерами горожан и деньги не берет. Пока. Но если захочет, то помешать этому, не прибегая к административному давлению, не удастся. Законодательная коллизия в том, что МГТС вполне может стать вторым РАО «ЕЭС». Только отключения будут не веерные, а тех, кому и так не повезло.

Просто поразмышляем

Жизнь меняется так быстро, что за ней не успеваешь. Информационное пространство, появившееся вдруг, или телекоммуникационная среда не имеют границ, здесь все совершается мгновенно и бесконтрольно. Одним нажатием кнопки можно сделать практически ВСЕ — изменить орбиту спутника, остановить работу завода и даже... убить человека.

Правоохранительные органы на Западе уже зарегистрировали первое убийство через Интернет. Да, Интернет себя еще покажет, и не зря его пишут с большой буквы. Этот параллельный мир подвластен лишь немногим. И преступления там совершаются не угрюмыми урками с заточками, а стрижеными пацанами, жующими резинку, которых нередко нанимают авторитеты. Например, в настоящее время управлением «Р» МВД России ведется следствие по делу вмешательства в коммуникационные сети «Газпрома», которое привело к тому, что вывело из строя всю систему этого монополиста. Это совершили несколько 16-летних подростков по «просьбе» крутых заказчиков, передавших им коды доступа в систему. Мальчишки вошли и поместили там 24 программы типа «троянский конь», позволяющие перехватить управление газовыми потоками. В результате центральный командный пульт оказался под внешним контролем.

Интернет-преступления растут, как снежный ком. Если в 1997 г. в России было зарегистрировано 17 преступлений в сфере компьютерной информации, то в 1998-м их было уже 67, а в 1999-м — 852! И деньги там крутятся НЕМЕРЕННЫЕ. Например, управлением «Р» недавно была перехвачена контрабандная поставка спецтехники на сумму 1,7 миллиона долларов. Сыщики долго сидели в засадах, ожидая гонцов, звонков, предложений, но... за партией никто не пришел. Ее просто списали, как «мелочь»!

Надо честно признать, что общество пока не готово блокировать весь огромный спектр подобных деяний. Мы недавно приняли «свежий» Уголовный кодекс с новой главой о компьютерных преступлениях, но сегодня он уже перестал соответствовать хитроумной смекалке криминальных кулибиных, и правоохранительные органы говорят о необходимости доработки закона.

Но, как бы ни изощрялись юристы, нищие и образованные инженеры, оставшиеся без работы, всегда найдут лазейку, чтобы обойти закон и заработать тысячу-другую баксов.

Человеку, далекому от высоких технологий, трудно представить безграничные возможности хакеров и фрикеров. Пока на слуху лишь пострадавшие от самых простых преступлений. Например, Европу всколыхнул случай, разбиравшийся в пражском суде. Пожилой супружеской паре пришел колоссальный счет за международные телефонные переговоры по... эротической линии. А муж, между прочим, парализован, и жена почти не слышит.

По данным управления «Р» МВД России, наша страна выплатила Вьетнаму в прошлом году в одностороннем порядке 2,5 миллиона долларов, расплачиваясь за незаконные переговорные пункты, использующие аппаратуру подстановки ложного телефонного номера в режиме кабельной телефонии.

Плод работы фрикеров — клонированные телефоны-двойники, когда к одному номеру сотового телефона подключаются до ста (!) абонентов. «Черный» рынок услуг связи предлагает также пользователям так называемый «вечный» пейджер. Это когда на один номер клонируются десятки клиентов, каждый из которых имеет свой пароль. По оценкам международных организаций, ущерб от противоправной деятельности в сфере телекоммуникаций оценивается в 13 млрд. долларов США в год.

Пока в нашей стране сетями пользуются лишь менее четырех процентов россиян. Не выходя из дома, вы можете переслать в любую точку сто долларов, а можете — сто миллионов долларов. Можно заказать пиццу (и через полчаса вам ее принесут), а можно — купить виллу на остро-

вах. Заходя в Интернет, вы видите, КАКИЕ услуги там предлагаются. Все, что угодно! На любой вкус, в том числе криминальный. Глядя на экран телевизора, где умненький паренек, пробежав по клавишам, обставляет солидных дядей, мы подчас умиляемся. Не пройдет и десяти лет, как эти парни будут держать весь мир под контролем. Мы готовы к этому?

Флай

Сотрудники управления по борьбе с преступлениями в сфере высоких технологий МВД РФ (управление «Р») задержали торговца сверхсекретными прослушивающими устройствами «Флай». С их помощью можно незаметно подключаться к телефонным сетям на территории бывшего СССР, в том числе прослушивать линии связи правоохранительных органов и спецслужб. В конце прошлого года оперативники управления «Р» получили информацию, что на московском черном рынке появились прослушивающие устройства «Флай». Поскольку прибор является секретным, сыщики занялись розысками продавца. Вскоре они вышли на 57 летнего директора столичной торговой фирмы. Предпринимателя взяли под наблюдение, а на днях задержали с поличным. Сделка должна была состояться в офисе бизнесмена в Сокольниках. Во время передачи прибора покупателю, который готов был выложить за него $4,5 тыс., на руках продавца защелкнулись наручники. Проведя обыски в офисе и квартире задержанного, оперативники обнаружили еще несколько таких устройств.

Прослушивающее устройство «Флай» было разработано несколько лет назад в одном из закрытых НИИ. Небольшой прибор (обычно его маскируют под телефон с АОНом или монтируют в кейс) обладает уникальными характеристиками. Он позволяет подключиться практически к любому междугороднему каналу связи на территории бывшего СССР, через него выйти на интересующего абонента (пользователя местной городской телефонной сети) и прослушивать его разговоры. Особая ценность этой «прослушки» состоит в том, что работу «Флая» практически невозможно обнаружить, даже если применить спецаппаратуру. Уникальный прибор пошел «в народ» несколько лет назад, после того как один из бывших сотрудников НИИ-разработчика выпустил брошюру, где указал ряд характеристик устройства и другую информацию, необходимую для изготовления «Флая». Часть тиража попала на черный рынок, прибор вызвал живой интерес у преступных группировок и коммерческих фирм, занимающихся незаконным прослушиванием. Были привлечены оставшиеся без работы или получающие мизерные зарплаты специалисты оборонных предприятий. Поскольку для производства «Флая» не нужно иметь уникального оборудования, а большая часть используе-

мых в этом приборе комплектующих доставляется из-за рубежа, умельцы быстро наладили производство «прослушек». По оценкам сотрудников управления «Р», сейчас в незаконном обороте находятся десятки таких приборов. Как правило, сами изготовители «Флая» им не торгуют, а передают торговцам-посредникам. Именно один из таких продавцов и был взят с поличным. Сейчас оперативники устанавливают, кто конкретно но изготовил изъятые прослушивающие устройства.

Краткая хроника истории органов и войск правительственной связи

1918–1941 гг.

Март 1918 года — Переезд правительства Республики (СНК РСФСР) и руководства партии (ЦК РКП(б)) из Петрограда (из Смольного) в Москву (в Кремль).

Сентябрь 1918 года — В телефонной комнате Кремля установлен 100-номерный коммутатор ЦБ-100/20.

1918 год — М.В. Шулейкин теоретически обосновал возможность организации высокочастотной связи по проводам.

Август 1920 года — Выходит проект Положения об отделе связи Кремля.

Май 1921 года — Постановлением Малого Совнаркома при ВЧК создан Специальный отдел под руководством Г.И. Бокия — криптографическая служба страны.

1921 год — Первые опыты по многоканальному телефонированию на заводе «Электросвязь» в Москве под руководством В.М. Лебедева.

Январь 1922 года — Завершены работы по установке в Кремле автоматической телефонной станции.

1923 год — П.В. Шмаков и В.А. Куприянов практически подтвердили возможность ВЧ-телефонирования.

1929 год — При одном из управлений ОГПУ создано отделение правительственной связи.

1930 год — Сданы в эксплуатацию первые линии ВЧ-связи Москва-Ленинград и Москва-Харьков.

Июнь 1931 года — Приказом ОГПУ №308/183 от 10 июня 1931 года сформировано 5-е отделение Оперативного отдела ОГПУ с целью создания и эксплуатации междугородной правительственной телефонной связи.

1930-е годы: Строительство магистральных воздушных линий связи, использовавшихся прежде всего для нужд междугородной правительственной ВЧ-связи, оборудование территориальных и региональных ВЧ-станций.

1934 год — На заводе «Красная Заря» (Ленинград) закончена разработка и начался крупносерийный выпуск трехканальной аппаратуры высокочастотного телефонирования СМТ-34 (система многоканального телефонирования 34-го года), работающей в диапазоне 10,4 — 38,4 кГц и обеспечивающей удовлетворительное качество связи на расстоянии до 2000 км.

1935 год — На базе отдела ВЦИК образован отдел технической связи Управления коменданта Московского Кремля (под руководством Г.Д. Любимова).

1935-1936 годы: На заводе «Красная Заря» в Ленинграде разработано первое отечественное устройство автоматического засекречивания телефонных переговоров — инвертор ЕС (К.П. Егоров и Г.В. Старицын) и налажен его выпуск.

1936 год — Образованы отдел связи Главного управления охраны (ГУО) НКВД (под руководством П.А. Потапова) и отдел связи Хозяйственного управления (ХОЗУ) НКВД (под руководством Н.А. Болдова).

Январь 1938 года — Постановление СНК СССР №53/ко от 5 января 1938 года «О развитии правительственной ВЧ связи».

Апрель 1938 года — Постановление СНК СССР №454-97сс от 9 апреля 1938 года «О развитии правительственной высокочастотной связи».

Ноябрь 1938 года — Постановление СНК СССР №1240-300сс от 17 ноября 1938 года «О развитии правительственной высокочастотной связи».

Январь 1939 года — в состав отдела связи Управления коменданта Московского Кремля Комендатуры Московского Кремля входят:

- автоматическая правительственная телефонная станция;
- автоматическая кремлевская телефонная станция;
- междугородняя станция;
- военный коммутатор;

- кросс;
- бюро повреждений;
- аккумуляторная и генераторная установки;
- справочный стол;
- линейное хозяйство;
- радиослужба;
- часовое хозяйство;
- служба охранной связи и сигнализации;
- мастерская;
- склады.

Апрель 1941 года — на апрель 1941 года аппаратура простого засекречивания стоит на 66 из 134 связей правительственной ВЧ связи.

Начало 1941 года — На магистрали Москва-Ленинград установлена 20-канальная аппаратура ВЧ-телефонирования.

Май 1941 года — Распоряжением СНК СССР №5-рс от 6 мая 1941 года утверждено «Положение о порядке эксплуатации правительственной ВЧ связи».

Май 1941 года — Советом Народных Комиссаров (СНК) СССР утверждено Положение о правительственной связи СССР, засекреченная ВЧ-связь отнесена к категории правительственной связи.

Июнь 1941 года — К началу Отечественной войны ВЧ телефонная связь была организована с большинством столиц союзных республик, многими областными центрами, военными округами.

1941–1945 гг.

Июнь — декабрь 1941 года В интересах обороны страны организована ВЧ-связь с районами формирования новых и резервных армий, с основными заводами оборонной промышленности по производству вооружений и военной техники, с базами комплектования и снабжения действующей Красной Армии. Из Ленинграда в Уфу эвакуированы лаборатории НИИ связи и цех дальней связи завода «Красная Заря», которые развернули работы по разработке и выпуску новой каналообразующей и коммутационной техники, специальной аппаратуры и средств защиты, в том числе и полевых малогабаритных образцов.

Центральная станция ВЧ-связи перенесена в защищенное место — на платформу станции московского метро «Кировская».

Октябрь 1941 года — на базе отделения 4 спецотдела НКВД СССР создан Отдел правительственной ВЧ-связи НКВД СССР.

Декабрь 1941 года — При фронтах создаются отделы, а при армиях — станции ВЧ-связи с непосредственным подчинением их Отделу правительственной связи НКВД СССР (начальник — полковник И.Я. Воробьев).

Январь 1942 года — Постановлением Государственного Комитета Обороны (ГКО) на НКВД было возложено эксплуатационное обслуживание и охрана магистральных линий и проводов, используемых для связи Ставки с фронтами и армиями.

Январь 1943 года — постановлением ГКО строительство, восстановление, эксплуатационное обслуживание и охрана всех магистральных линий, используемых для правительственной ВЧ-связи между СВГК и штабами фронтов и армий были возложены на НКВД СССР. В составе ГУВВ сформировано управление связи (войск правительственной связи) а принятые от ГУСКА 135 отдельных линейно-строительных рот связи сведены в 12 отдельных полков, 4 отдельных батальона и отдельные автотранспортную и аэросанную роты общей численностью более 31 тыс. человек.

Февраль 1943 года — Строительство и восстановление линий связи также возложено на НКВД СССР, для чего в его составе образуется Управление связи с подчиненными ему специальными воинскими частями (начальник — генерал-майор войск связи П.Ф. Угловский) июнь.

1943 года — создано Управление войск правительственной ВЧ-связи НКВД СССР.

1943 год: Организация и обеспечение оперативной, защищенной и бесперебойной работы ВЧ-связи Ставки ВГК, Генштаба, ЦК ВКП(б), СНК СССР с командованием фронтов и армий, органами власти на местах, важнейшими оборонными объектами и предприятиями промышленности, органами государственной безопасности и внутренних дел полностью возложены на Отдел Правительственной связи НКВД СССР и Управление войск Правительственной связи НКВД СССР (создано в июле 1943 года), которые курировал замнаркома внутренних дел комиссар госбезопасности 2 ранга И.А. Серов.

1941–1945 годы: За годы войны войсками правительственной связи во взаимодействии со связистами Красной Армии и Наркомата связи, зачастую в боевой обстановке, было построено и восстановлено 66 500

км воздушных линий, подвешено и восстановлено 363 200 км медных и стальных проводов, построено 33 800 км шестовых линий. Успешно решены задачи по обеспечению ВЧ-связью советских делегаций на Тегеранской и Ялтинской конференциях.

В мае 1945 года (конец войны с Германией) протяженность обслуживаемых войсками линий ВЧ связи составила 32944 км, а в августе 1945 года (во время боевых действий против Японии) достигла 36854 км.

Октябрь 1945 года — Приказом НКВД СССР №001185 от 10 октября 1945 года «О расформировании частей войск правительственной связи» в соответствии с Постановлением СНК СССР №2417-643 от 21 сентября 1945 года «О сокращении численности войск НКВД» расформирован ряд отдельных частей и подразделений войск правительственной ВЧ-связи, ряд отдельных бригад переформирован в полки, а отдельные батальоны — в роты.

1945–1946 годы — перед войсками правительственной связи и Отделом правительственной связи поставлена задача обеспечения правительственной связью командования групп советских войск, дислоцирующихся на территории Восточной Германии, Венгрии, Австрии, Польши, Чехословакии, Румынии, Монголии, кроме того в 1945–1946 годах отремонтировано 1965 км линий, заменено 77000 тыс. км проводов рабочих и служебных цепей и укреплено более 36000 опор.

1946–1947 годы — Отдел технической связи Управления коменданта Московского Кремля и Отдел связи Главного управления охраны (ГУО) МГБ объединены в Отдел связи ГУО МГБ (П.А. Потапов), на который возложена ответственность за городскую правительственную связь в Москве.

1947 год — для нужд ГУО МГБ создана система дуплексной подвижной радиосвязи «Интеграл-Градиент» (устанавливалась на автомобилях) и система радиоподвижной связи «Красная площадь» (для обеспечения радиосвязью мероприятий на Красной площади и в других местах).

Август 1947 года — совместным приказом МВД и МГБ №00877/00458 от 26 августа 1947 года Отдел правительственной ВЧ-связи МВД СССР и Управление войск правительственной ВЧ-связи МВД СССР переданы в ведение МГБ СССР.

1948 год — с введением в действие АТС городской связи машинной системы емкость служебной телефонной сети Кремля увеличена на 1000 номеров.

1951 год — к середине 1951 года на территории СССР и за границей функционировали 223 ВЧ-станции (199 и 24 соответственно), обслуживавшие 2904 абонента (2465 и 439 соответственно).

1951 год — в центральном аппарате ОПС МГБ по штату 371 сотрудник, территориальные органы правительственной связи составляют 18 отделов, 111 отделений и 155 групп, в которых по штату 2174 человека, за границей 5 отделов и 1 отделение правительственной связи штатной численностью 294 человека.

Октябрь 1951 года — по Приказу МГБ СССР №00764 от 18 октября 1951 года части войск правительственной связи на территории СССР реорганизованы в части правительственной ВЧ-связи Внутренней охраны МГБ, при этом отдельные полки, батальоны и роты правительственной связи переформировывались в отдельные отряды, дивизионы и команды правительственной ВЧ-связи внутренней охраны МГБ.

1952 год — Отдел связи ГУО выведен из ГУО и включен в состав ОПС МГБ.

1952 год — в составе УВПС МГБ СССР на территории страны — 4 отдельных отряда, 7 отдельных дивизионов и 11 отдельных команд правительственной ВЧ-связи внутренней охраны МГБ, за границей — 4 отдельных полка и 18 отдельных рот войск правительственной связи МГБ.

Март 1952 года — Приказом МГБ СССР №00182 от 14 марта 1952 года Управление войск правительственной ВЧ-связи МГБ реорганизовано в Управление частей правительственной ВЧ-связи Главного управления внутренней охраны МГБ.

Май 1951 года — Управление войск правительственной ВЧ-связи МГБ СССР переименовано в Управление частей правительственной связи Главного управления внутренней охраны (ГУВО) МГБ СССР.

Март 1953 года — в составе объединенного Министерства внутренних дел СССР созданы Отдел «С» МВД (бывший отдел правительственной ВЧ-связи) и Отдел частей ВЧ-связи Главного управления внутренней охраны МВД.

1954 год — емкость правительственной АТС (ПАТС) в Кремле составляет 3500 номеров за счет установки коммутационного оборудования декадно-шаговой системы отечественного производства на 1000 номеров.

1954 год — внедрена 4-канальная система подвижной радиосвязи «Ай-Петри-Памир» с закрытием информации и дальностью радиосвязи без переприема 50–60 км.

1954 год — штатная численность войск правительственной связи составляет 8021 единиц.

Март 1954 года — при создании КГБ при СМ СССР отдел «С» передан в его состав, а Отдел частей правительственной ВЧ-связи остался в составе Главного управления внутренней и конвойной охраны МВД.

Сентябрь 1954 года — Распоряжением Совета Министров СССР №10709рс от 25 сентября 1954 года части ВЧ-связи внутренних войск и внутренней охраны МВД переданы в ведение КГБ при СМ СССР.

Сентябрь 1954 года — Отдел войск правительственной ВЧ-связи с подчиненными ему частями передан в ведение КГБ СССР, с присвоением ему условного наименования в/ч 9737.

Октябрь 1954 года — Приказом КГБ №00708 от 26 октября 1954 года отдельные полки правительственной ВЧ-связи ВВ МВД и отдельные дивизионы правительственной ВЧ-связи внутренней охраны МВД переименованы в отдельные полки и отдельные батальоны войск правительственной ВЧ-связи.

Декабрь 1954 года — части ВЧ-связи переданы из МВД в КГБ 1955 год — на войска правительственной связи возложено обеспечение связью командования Объединенных вооруженных сил стран-участниц Варшавского договора во время проводимых учений и спецмероприятий.

1956 год — Постановлением СМ СССР №333-210сс от 13 марта 1956 года ввиду того, что количественный состав войск правительственной связи не соответствовал мобилизационным планам развертывания частей в военное время, их численность была увеличена на 13000 единиц и должна была быть доведена к 1958 году до 21846 единиц, что позволило бы содержать 13 отдельных полков и 11 отдельных батальонов правительственной связи.

Июнь 1959 года — Отдел «С» КГБ при СМ СССР объединен с Отделом войск правительственной связи КГБ при СМ СССР в единый Отдел правительственной связи (ОПС) КГБ при СМ СССР, территориальные отделы и отделения «С» преобразованы в отделы и отделения правительственной связи.

Август 1959 года — Приказом начальника войск правительственной связи №0137 от 17 августа 1959 года отдельные полки, батальоны и роты войск правительственной ВЧ-связи стали именоваться отдельными полками, отдельными батальонами и отдельными ротами войск правительственной связи КГБ.

Июль 1959 года — 9 июля 1959 года объявлен новый штат Отдела правительственной связи, в соответствии с которым создан Штаб войск правительственной связи.

Февраль 1960 года — в соответствии с Постановлением ЦК КПСС и СМ СССР от 5 февраля 1960 года численность войск правительственной связи сокращена на 4168 единиц.

Март 1960 года — Приказом КГБ №00109 от 16 марта 1960 года установлено количество отдельных полков правительственной связи на территории СССР — 15.

Октябрь 1960 года — Постановлением СМ СССР №1102–455 от 15 октября 1960 года предусмотрена организация правительственной ВЧ-связи до командиров бригад ракетных войск, командиров дивизий противовоздушной обороны, командиров дивизий и бригад ракетных подводных лодок включительно, для чего необходимо в течение 1961–1965 годов организовать до 50 новых ВЧ-станций.

1960 год — к Отделу правительственной связи (ОПС) КГБ при СМ СССР присоединен отдел связи Хозяйственного управления КГБ.

Июль-август 1960 года — части войск правительственной связи, дислоцирующиеся за границей, объединены с соответствующими отделами правительственной связи под общим командованием, созданы отделы правительственной связи при группах советских войск.

1960 год — за границей для обеспечения связи с группами войск дислоцируется ряд частей и подразделений войск правительственной связи: ГДР — 3 батальона, 2 узла, ПНР — 4 батальона, 1 узел, ВНР — 1 узел, 6 рот, МНР — 1 батальон.

1963 год — разработана и изготовлена система радиосвязи на Красной площади «Север» для связи оперативного состава в ходе мероприятий на Красной площади и в других местах.

1967 год — вступила в действие дуплексная радиоподвижная ультракоротковолновая незасекреченная система связи «Роса» (в конце 1960-х годов в автомобилях абонентов высшей категории установлена засекречивающая аппаратура временной стойкости).

1967–1968 годы — проведены работы по внедрению в полевую сеть правительственной связи аппаратуры засекречивания временной стойкости «Коралл» и гарантированной стойкости «Лагуна».

1968 год — на конец 1968 года в сеть автоматической телефонной правительственной связи включено 184 населенных пункта, а с остальными объектами, оборудованными ВЧ-связью, связь организована по заказной системе.

1960-е годы — положено начало внедрению мер по защите обслуживаемых подразделениями Московского узла правительственной связи технических средств от возможной утечки информации.

1960-е годы: в странах социалистического лагеря организованы свои сети правительственной связи, для чего им передана станции и аппаратура ВЧ-связи и аппаратура засекречивания, шифры для которой изготовлялись в СССР и направлялись к местам назначения диппочтой.

1969 — по настоящее время

1969 год — на базе ОПС КГБ при СМ СССР создано Управление правительственной связи КГБ при СМ СССР.

1969 год — на основе служб Московского узла правительственной связи ОПС сформирован 3-й отдел УПС (Московский отдел правительственной городской связи), на который возложены задачи организации и обслуживания стационарных и абонентско-кабельных средств городской правительственной и служебной связи, систем звукоусиления, перевода речей, телевидения и часификации на правительственных и специальных объектах в Москве.

1973 год — организована правительственная связь с самолетом во время дальних перелетов во время визита советского руководства из СССР в США.

1978 год — введена в эксплуатацию выделенная система правительственной городской автоматической телефонной связи для высшей категории абонентов на 1000 номеров, получившая наименование АТС-1, а существующая сеть городской правительственной связи (ПАТС) емкостью 5000 номеров переименована в АТС-2.

1970-е годы — в правительственных сетях телефонной связи осуществлен переход на использование телефонных аппаратов, разработанных по специальным требованиям.

1979 год — Постановлением ЦК КПСС и СМ СССР №558-183 от 13 июня 1979 года утверждено новое «Положение о правительственной связи», в соответствии с которым правительственная связь в СССР создавалась:

- международная;
- междугородная;
- городская (Москва и Московская область);
- с подвижными объектами;
- полевая.

1980 год — емкость АТС-2 доведена до 6000 телефонных номеров.

1982 год — на базе зарубежного квазиэлектронного оборудования емкость АТС-1 увеличена до 2000 номеров.

Ноябрь 1983 года — Приказом КГБ СССР №0036 от 5 ноября 1983 года утверждено «Наставление по организации правительственной связи в операциях Вооруженных сил СССР».

1983 год — в Кремле введена в действие отечественная квазиэлектронная станция для сети правительственной связи АТС-2, а емкость сети АТС-2 составила 7000 номеров в Москве и 10000 номеров по стране (с учетом зонных станций).

1985 год — в целях повышения оперативности и надежности управления полевой сетью правительственной связи в мирное и военное время созданы управления войск правительственной связи на театрах военных действий (стратегических направлениях, всего 4).

1989–1992 годы — осуществлен вывод частей правительственной связи из Чехословакии, Венгрии, Монголии, Польши и Восточной Германии.

Август 1991 года — Указом Президента СССР №УП-2484 от 29 августа 1991 года на базе отделов и служб УПС КГБ создан Комитет правительственной связи (КПС) при Президенте СССР.

Декабрь 1991 года — Указом Президента РФ №313 от 24 декабря 1991 года на базе бывших Восьмого главного управления КГБ, Шестнадцатого управления КГБ и Комитета правительственной связи при Президенте СССР, а также ряда научных и производственных организаций, Указом Президента РФ №313 от 24 декабря 1991 года создано Федеральное Агентство Правительственной Связи и Информации (ФАПСИ) при Президенте России.

1992 год — на базе отделов и отделений правительственной связи местных управлений бывшего КГБ СССР сформированы Центры правительственной связи (ЦПС) четырех категорий.

Февраль 1993 года — принят Закон РФ «О федеральных органах правительственной связи и информации».

Февраль 1993 года — на базе Орловского Военного института правительственной связи (ВИПС) открыт для посещения Музей правительственной связи.

Октябрь 1996 года — Музей правительственной связи преобразован в Музей ФАПСИ.

1997 год — правительственной связью охвачено около 300 городов и спецобъектов, телефонная связь предоставлена более 20 тысячам абонентов, документальной связью охвачено свыше 1600 органов власти и различных организаций, в 79 городах функционируют комплексы радиосвязи с подвижными объектами, которые обслуживают свыше 3 тысяч абонентов.

Знаменательные даты и праздники

- 15 февраля — День войск правительственной связи (1943 год);
- 5 мая — День рождения криптографической службы (1921 год);
- 1 июня — День органов правительственной связи (1931 год).

Структуры отделов

Отдела правительственной ВЧ-связи (май 1942 года):

- руководство;
- секретариат;
- 1 отделение (эксплуатация связи);
- 2 отделение (развитие и строительство ВЧ-связи);
- 3 отделение (радиосвязь);
- 4 отделение (линейная эксплуатация);
- 5 отделение (кадры);
- 6 отделение (материально-техническое снабжение);
- спецлаборатория.

Отдел связи Главного управления охраны МГБ (1947 год):

- кабельное отделение;
- линейное отделение;
- отделение загородных линейно-кабельных сооружений;
- отделение АТС;
- радиоотделение;
- киногруппа.

Отдел «С» КГБ при СМ СССР (1957):

- Центральный узел правительственной связи (ЦУПС);
- 1-е отделение (ВЧ-связи территориальных органов);
- 2-е отделение (линейно-аппаратных залов и автоматической междугородной телефонной станции);
- 3-е отделение (засекречивающей аппаратуры);
- 4-е отделение (зонных станций правительственной связи);
- Московский узел правительственной связи (МУПС);
- 5-е отделение (АТС, ЭПУ, кроссов, часификации);
- 6-е отделение (абонентских средств);
- 7-е отделение (радиосвязи и звукоусиления);
- 8-е отделение (линейно-кабельных сооружений).

Часть 1. Классификация

Принципы построения и функционирования проводных систем связи и коммутации

Исторический обзор

Конец прошлого века ознаменовался рядом революционных технических открытий и изобретений. Одним из них было изобретение в 1876 г. Беллом телефонного аппарата и телефонной связи. Предприимчивые американцы, незамедлительно, в 1878 г. в городе Нью-Хевене стали строить первую в мире ручную телефонную станцию. Естественно, для увеличения надежности телефонной связи, ее удешевления, тут же начали пытаться автоматизировать процесс установления и обслуживания соединений. Было предложено много разных проектов построения Автоматических Телефонных Станций (АТС), однако, не так много оказались достаточно надежными, получившими народное признание.

В 1889 г., господину Строуджеру (почему-то опять из США) пришла идея создания декадно-шагового искателя (ДШИ). России настолько понравилось изобретение г. Строуджера, что до сегодняшнего дня около 25% парка московской ГТС — это АТС декадно-шагового типа (АТС ДШ). Типичный декадно-шаговый искатель, это довольно сложное электромеханическое устройство, этакое продвинутое электромеханическое реле, ориентированное на передачу и преобразование информации о вызываемом номере в виде декадных шлейфовых импульсов тока. Стандартно, ДШИ имеет 2 электромагнита, подавая последовательно на которые от 1-го до 10 импульсов тока можно осуществить выбор одного из 100 доступных шнуров (коммутируются не только разговорные провода, поэтому ДШИ коммутирует больше, чем просто 2 провода от Вашего телефонного аппарата). Поскольку ДШИ имеет механические контакты, которые постоянно движутся, то их износ и окисление приводит к тому, что сопротивление в месте контакта со временем повышается. Все бы ничего, но мощные электромагниты ДШИ вызывают вибрацию стоек, в которых их установлено очень много, что в свою очередь приводит к тому, что эти контакты имеют к тому же и переменное сопротивление. Как следствие — в процессе разговора появляются

посторонние трески и шумы, являющиеся смертью для современных систем передачи дискретной информации (например модемов).

В 1914 году Бетлаундер (на этот раз Швеция) изобрел многократный координатный соединитель (МКС). Так появились АТС координатного типа (АТСК). Этих в Москве еще больше — около 40%. Одним из достоинств МКС является то, что в процессе установления соединения контакты МКС не трутся друг о друга при замыкании, а замыкаются как в стандартном электромеханическом реле (контакты давления). Поскольку трение скольжения всегда больше трения качения, то изобретение МКС, в каком то смысле, аналогично изобретению колеса. Контакты значительно меньше изнашиваются, механических вибраций меньше, качество связи выше. В 1939 году в США была введена в эксплуатацию первая АТСК. Целых 25 лет потребовалось с момента изобретения МКС. Это связано с тем, что в АТСК производится довольно сложная обработка управляющей информации. В первых станциях это делалось исключительно на реле.

В стройном ряду аналоговых станций стоят еще и так называемые квази-электронные и электронные станции. Коммутация в таких станциях осуществляется с помощью герметизированного контакта (геркон) или электронного ключа, а управлением ведает микропроцессор. Революционное внедрение микропроцессоров сильно повысило эффективность АТС, позволило оснастить рядом приятных дополнительных функций (дополнительные виды обслуживания или ДВО). Современная АТС в частности и связь вообще немыслимы без микропроцессорной техники.

Однако, начиная со старика Белла и до электронных АТС, не менялся сам принцип коммутации сигнала — это всегда был аналоговый сигнал с пространственной коммутацией, а значит качество канала с увеличением точек коммутации падало, а каждая точка коммутации требовала соответствующего физического элемента, а, соответственно, и вся станция имела гигантские размеры. Ситуация кардинально изменилась с появлением цифровых АТС.

В 1933 г. В.А. Котельников сформулировал теорему, носящую теперь его имя. В 1938 г. А.Х. Риверс запатентовал тот метод преобразования аналоговых сигналов цифровой временной коммутации, который мы теперь называем ИКМ. Теорема Котельникова является краеугольным камнем цифровизации сигналов, а следовательно математической базой для работы цифровых АТС при передачи, в первую очередь, речи. К сожалению, на Западе то же самое связывают с именем Найквиста, ну да Бог им судья, отмечаем же мы День Радио с именем Попова, а не Маркони. Однако, Запад не дремал, и коварно использовав имя Найквиста

ввел в эксплуатацию в 1975 году первую в мире цифровую АТС типа E10 (это произошло во Франции) и через двадцать с небольшим лет после этого знаменательного события, в настоящее время, благополучно завершает реконструкцию своих сетей на базе цифрового стандарта.

В цифровой АТС сигнал коммутируется и передается в цифровом виде, то есть в виде последовательности нулей и единиц. Коммутация осуществляется, как правило, пространственно — временным способом. Именно появление интегральных коммутаторов от 256 до 4096 неблокированных каналов сделали цифровые методы коммутации доступными. Это всего лишь одна микросхема. Подробнее об интегральных коммутаторах можно посмотреть у фирм MITEL или SIEMENS. Стандартным объектом коммутации является цифровой канал со скоростью 64 кбит/сек. Более подробно о преобразовании аналогового речевого сигнала в цифровой речь пойдет ниже.

Важным достоинством цифровых АТС является то, что с помощью них можно очень легко передавать любые виды информации в цифровой форме, что очень сложно было сделать на аналоговых АТС, а это является необходимым условием создания ISDN (Integrated Services Digital Network или Цифровая сеть с Интегрированными Услугами) сетей. ISDN — это сеть связи, обеспечивающая полностью цифровые соединения между абонентскими устройствами для поддержания возможности передачи как речевых, так и неречевых данных с помощью стандартизированных многофункциональных интерфейсов. Это очень интересное и перспективное направление в развитии сетей связи, имеющее, однако, на сегодняшний день очень малое практическое значение, особенно для России.

Проблемы стандартизации в телефонии

Если Вы съедите нестандартный по форме бутерброд, то ничего не произойдет. Если вы будете писать нестандартной ручкой, то в этом так же нет ничего страшного. Если Вы оригинально (нестандартно) видите мир, то это даже хорошо — может быть из Вас получится модный писатель, журналист или модельер (если, конечно, не имеется в виду простой дальтонизм). Для связи же малейшая нестандартная работа отдельных узлов — и вот Вы уже никак не можете дозвониться любимой бабушке. Или Вы с ужасом думаете, как же этот прекрасный, красивый телефонный аппарат с маленькой, элегантной и надежной вилочкой RJ-11 подключить монстроидальной советской телефонной розетке. Увы никак, только с помощью хирургического вмешательства.

Для преодоления подобных смешных проблем, и проблем значительно более серьезных, связисты давно создали Международную консультативную организацию по телефонии (ITU-T). Когда еще в 1995 году специалисты рекомендовали Вам подождать с выбором высокоскоростного модема на скорость больше 20000 бит/сек, они на самом деле ждали утверждения стандарта V34. Значимость стандартизации в области связи трудно переоценить. Кратко, в духе нашего времени, можно сказать так. Если вы работаете в области связи, а тем более что-то разрабатываете и хотите заработать много денег — придерживайтесь стандартов, прежде всего национальных, а если их нет или они малодоступны, то международных. Почитать немного о стандартах в области телефонии можно на сервере ITU-T или на сервере Европейского института стандартизации в области связи. К сожалению, эта информация почему-то считается коммерческой.

Стандартизацией телефонии в России занимается Министерство связи и их головной институт в этом вопросе — ЛОНИИС. Первичным источником всех стандартов в России, в котором, впрочем, непосвященному человеку невозможно разобраться, является так называемый Руководящий Документ по построению Общегосударственной Системы Телефонной связи (ОгСТфС). Лицензию на проведение сертификационных испытаний (процедуры, призванной установить соответствие некоторого устройства стандартам) имеет и ряд других подразделений Министерства связи и ГосСтандарта. Однако мы настоятельно рекомендуем Вам, если у Вас будет такая потребность, пользоваться услугами ЛОНИИС. Там действительно работают высококлассные специалисты, да и по деньгам это не самый дорогой вариант.

Как устроен абонентский комплект

Для подключения оконечного аналогового телефонного устройства к телефонной станции используется аналоговая абонентская линия, имеющая более строгое название — Z-интерфейс. Именно сюда Вы включаете свой обычный телефонный аппарат с помощью 2-х проводов. Это патриарх телефонный связи. Стандарт на него сформировался еще в 30-е годы и с тех пор претерпел весьма незначительные изменения. На нем лежит отпечаток уровня техники и технологий тех лет. И, как часто это бывает, то что на уровне стародавних технологий реализовывалось сравнительно просто, а может быть и вообще было единственным разумным способом реализации, через некоторое время превратилось в технологический архаизм. Однако, деваться некуда — существуют миллиарды абонентских устройств, работающих в этом стандарте.

Полный стандарт на Z-интерфейс содержит достаточно много информации. Например здесь мы привели только описание акустических и вызывных сигналов для абонентской линии.

Остановимся на ключевых моментах.

Для передачи и приема речевой информации используются всего 2 провода. По ним же осуществляется дистанционное питание оконечного абонентского устройства и вся сигнализация — трубка снята, трубка опущена и набор номера. Согласно требованиям на телефонные аппараты абонентская линия должна обеспечивать ток не менее 18 мА. Для создания такого тока используется станционная линейная батарея с номинальным значением напряжения -60В или -48В. Легко заметить, что чем больше напряжение станционной батареи, тем более длинные абонентские линии будут поддерживаться. Для рационального использования энергоресурсов, уменьшения тепла, выделяемого в абонентских комплектах и увеличения допустимой длины абонентской линии современные АТС используют схемы со стабилизацией тока питания абонентского шлейфа. Номинальное значение тока, в этом случае, обычно делается равным 25–30 мА. Замыкание/размыкание абонентского шлейфа, с помощью контакта телефонного аппарата, используется и для передачи информации в станцию о том что трубка телефонного аппарата снята и о наборе номера.

Другой непременный атрибут абонентской линии — электрическая симметрия проводов. В общем случае, для количественной оценки симметрии служит так называемый коэффициент затухания асимметрии. Это частотно зависимый параметр, нормируемый в области полосы рабочих частот. Чем больше коэффициент затухания асимметрии, тем менее абонентская линия чувствительна к внешним помехам. Следствием недостаточной симметрии абонентской линии является прослушивание посторонних сигналов — других разговоров, фона переменного тока 50 Гц, канала радиотрансляции и т.д. Для выполнения данного параметра электрическая схема абонентского комплекта должна обеспечивать достаточно высокий модуль комплексного сопротивления каждого из проводов относительно земли во всем диапазоне рабочих частот.

В первых АТС коммутация разговорного тракта осуществлялась двумя проводами. Поэтому абонентская линия традиционно двухпроводная. То есть для передачи и приема информации используются одни и те же провода. Это еще и большая экономия меди. Однако, за все нужно платить. Платить приходится тогда, когда становится необходимостью к такой линии подключать 4-х проводные устройства, то есть устройства, в которых отдельно обрабатывается канал передачи и канал приема. Это и каналообразующая аппаратура и 4-х проводные схемы коммутации (все цифровые схемы работают по 4-х проводной схеме), да и, практически, любые современные абонентские устройства. Схема, которая преобразует 2-х проводную линию в 4-х проводную так и называется схема преобразования 2–4 или противоместной схемой. Обычно она выполняется на базе мостовой схемы. Одно плечо моста — 2-х проводная линия, противоположное плечо (или, в общем случае, одно из плеч моста) балансный контур, а диагонали моста — прием и передача 4-х проводной части. Балансный контур призван обеспечить балансировку моста и максимум затухания в 4-х проводной части со стороны передачи на сторону приема. Однако, учитывая то, что импеданс со стороны абонентской линии в общем случае величина переменная, достижение больших значений этого затухания не представляется возможным. Более того, этот импеданс является переменной величиной, изменяющейся как в процессе установления соединения, так и от одного соединения к другому.

С целью увеличения затухания в 4-х проводной части во всей полосе рабочих частот балансный контур рекомендуется делать с комплексным импедансом, поскольку в импедансе стандартной абонентской линии присутствует и реактивная составляющая. Нормируется, однако, не импеданс балансного контура а входное сопротивление абонентского комплекта, которое является, в общем случае, производным от первого.

Конечное затухание между каналами приема и передачи в 4-х проводной части приводит к появлению так называемого электрического эха. Это создает ряд очень крупных проблем для телефонной связи, которые решаются в разных случаях по разному. Например в современных модемах, где очень важно иметь хорошее разделение между каналами приема и передачи в дополнение к описанной выше схеме делается так называемый эхокомпенсатор. Для спутниковых каналов, где временная задержка распространения сигнала достигает сотен миллисекунд и больше и эхо становится уже заметным для слуха человека, так же устанавливаются эхокомпенсаторы или, что хуже, эхозаградители.

Абонентский комплект должен обеспечивать посылку в абонентскую линию сигнала так называемого индукторного вызова, представляющего собой переменное напряжение синусоидальной или достаточно близкой к синусоидальной формы с частотой 25 Гц и действующим значением 95В. Попытки упростить вызывное устройство путем подачи вызывного напряжения частотой 50 Гц или используя чисто прямоугольный сигнал несут собой возникновение ряда неприятных последствий в ряду которых наиболее серьезным является отказ абонентского устройства распознать такой вызывной сигнал.

Генератор индукторного вызова современной АТС, полностью соответствующий всем требованиям, является довольно сложным устройством. В АТС «ЛОБЬ», например, для этой цели используется отдельный процессор. Во первых, требуется обеспечить сигнал, довольно близ-

кий к синусоиде, при достаточно точной частоте генерации. Ну и конечно, при всем при том, хочется избежать подстроечных элементов. Цифровой синтез сигнала при этом не имеет альтернатив. Есть еще определенные нюансы в построении этого генератора, которые вообще не оставляют шансов аналоговым генераторам (например на базе моста Вина).

Для решения описанных выше проблем при разработке схем современных абонентских комплектов существует целый класс микросхем, выполненных как правило по гибридной технологии, имеющих общее название SLIC (Subscriber Line Interface Circut). Если Вы никогда не разрабатывали абонентских комплектов на дискретной логике и у Вас есть необходимость быстро и хорошо это сделать, то Вам имеет прямой смысл использовать что-то вроде MH88612 или MH88617 от фирмы MITEL. Сама элементная база абонентского комплекта (собственно — одна эта микросхема) обойдется Вам в 3–4 раза дороже, чем аналогичный комплект на дискретной логике, однако позволит быстро получить гарантированно полноценно работающую схему.

В абонентский комплект современных цифровых АТС, кроме схемы преобразования 2–4, входит и устройство, обеспечивающее преобразование аналогового канала в цифровой и обратно. Такое устройство функционально состоит их следующих элементов: фильтр и кодер в канале преобразования A-D и декодер с фильтром в канале преобразования D-A. Фильтр, является необходимым компонентом для формирования канала с полосой пропускания 0.3 .. 3.4 кГц, являющегося стандартным для телефонной связи, ну и необходимым согласно теореме тов. Котельникова. Все описанные здесь функции современная элементная база реализует на одной микросхеме, называемой обычно кофидеком. Частота дискретизации в современной телефонии выбрана равной 8 кГц. Число уровней квантования — 256 (8 разрядов). Таким образом современный кофидек создает цифровой поток со скоростью 64 кбит/сек. Кодирование аналогового сигнала, используемое в телефонии, принято называть ИКМ (Импульсно-Кодовая Модуляция) или PCM (Pulse Code Modulation) кодированием

Подсчитано, что стандартный АЦП должен иметь примерно 12 разрядов для передачи речи с требуемым в телефонии качеством. Тем не менее кофидеки обходятся восьмью при том же, практически, качестве. Это достигается путем компандирования входного сигнала, то есть шкала преобразования кофидеков нелинейная. Существуют, A и МЮ законы компандирования, являющиеся стандартами, соответственно, для Европы и Америки. Стандартом на первичный цифровой канал 64 кбит/сек для России (ITU-T) является так же инверсия нечетных бит.

Для АТС «ЛОБЬ» было разработано три типа абонентских плат. Наиболее старые использовали трансформаторный абонентский комплект на дискретных элементах и кофидек MT8965 фирмы MITEL. Относительно новые используют тот же кофидек и слик MH88612 той же фирмы. Перспективные, те, для которых в настоящее время пишется программное обеспечение, будут использовать одну микросхему, содержащую в себе и СЛИК и кофидек фирмы National Semiconductor.

Непременным атрибутом абонентского комплекта являются элементы защиты от перенапряжений. Обычно их разделяют на 2 класса — элементы защиты от превышения тока и элементы защиты от превышения напряжения. Элементами защиты от тока являются токочувствительные элементы, резко увеличивающие свое сопротивление при превышении определенных значений токов в проводах абонентской линии. Это могут быть и обычные плавкие предохранители или так называемые термокатушки и автоматически восстанавливаемые современные элементы — позисторы. Для защиты абонентского комплекта от перенапряжений используются грозоразрядники или варисторы. Очень часто все эти элементы защиты устанавливаются не непосредственно в абонентском комплекте, а в кроссе АТС.

И еще одно замечание, которое необходимо учитывать при разработке абонентских комплектов на современной импортной элементной базе. Выбор СЛИКов, представляемых ведущими производителями, Mitel, Siemens, AMD, Motorola, National и др. просто огромен. Вместе с тем, большая часть из них рассчитана на питание станционной батареи 48В и более низкое, чем это принято в России, значение напряжения генератора индукторного вызова. Есть и еще ряд мелких проблем. Все это, к сожалению, сильно портит всю розовую картину телефонного изобилия.

Акустические и вызывные сигналы абонентской линии

При пользовании основными и дополнительными услугами абонентам могут передаваться из местных АТС следующие информационные акустические и вызывные сигналы:

- ответ станции;
- вызывной сигнал с частотой 25 Гц (прямой вызывной сигнал);
- контроль посылки вызова;
- занято;

- занято при перегрузке;
- указательный сигнал;
- сигнал вмешательства;
- сигнал уведомления;
- подтверждения приема (при заказе и отмене ДВО);
- сигнал ожидания (контроль посылки уведомления).

При пользовании основными и дополнительными услугами абонентам должны передаваться следующие акустические и вызывные сигналы:

- «Ответ станции» — информирует абонента о готовности станций к приему номера. Непрерывный синусоидальный сигнал частотой 425 ± 5 Гц. Номинальный уровень в точке с нулевым относительным уровнем минус 10 дБ, допустимые изменения уровня от минус 15 до минус 5 дБ. Второй акустический сигнал «ответ станции» непрерывный сигнал частотой 425 ± 3 Гц. Номинальный уровень в точке с нулевым относительным уровнем минус 10 дБ, допустимые изменения уровня от минус 15 до минус 5 дБ.
- «Посылка вызова» — информирует абонента о поступлении к нему вызова. Прерывистый синусоидальный сигнал частотой 25 или 50 ± 2 Гц, импульс 1,0 ± 0,1 с, пауза 4,0 ± 0,4 с. Первая посылка вызова не менее 0,3 ± 0,03. Напряжение на зажимах кросса должно быть 95 ± 5 В эф.
- «Контроль посылки вызова» — информирует вызывающего абонента о свободности вызывающего абонента и посылке ему вызывного сигнала, желательно посылать синхронно с сигналом посылки вызова. Прерывистый синусоидальный сигнал частотой 425 ± 3 Гц: импульс 1,0 ± 0,1 с, пауза 4,0 ± 0,4 с. Номинальный уровень в точке с нулевым относительным уровнем минус 10 дБ, допустимые изменения уровня от минус 15 дБ до минус 5 дБ.
- Сигнал «Занято» информирует абонента о занятости вызываемого абонента после набора номера или об отбое другого абонента после разговора, или при всех состояниях непроизводительного занятия. Прерывистый

синусоидальный сигнал частотой 425 ± 3 Гц: импульс 0,3 — 0,4 с, пауза 0,3 — 0,4 с. Номинальный уровень в точке с нулевым относительным уровнем минус 10 дБ, допустимые изменения уровня от минус 15 до минус 5 дБ.

- Сигнал «Занято при перегрузке» информирует вызывающего абонента об отказе в обслуживании из-за отсутствия свободных соединительных путей и станционных приборов. Прерывистый синусоидальный сигнал частотой 425 ± 3 Гц: импульс 0,15 — 0,2 с, пауза 0,15 — 0,2 с. Номинальный уровень в точке с нулевым относительным уровнем минус 10 дБ, допустимые изменения уровня от минус 15 до минус 5 дБ.
- «Указательный сигнал» информирует абонента о невозможности установления связи из-за устойчивой причины (отключение абонентской линии, изменение категории абонента). Последовательная передача трех частот: 1 = 950 ± 5 Гц, 2 = 1400 ± 5 Гц, 3 = 1800 ± 5 Гц. Частоты передаются в указанном порядке. Длительность импульса каждой частоты 0,33 ± 0,07 с, пауза между 1 и 2; 2 и 3 не более 0,03 с. Длительность интервала между посылками из трех частот = 1±0,25 с. Разность между уровнями соответствующих частот не должна быть более 3 дБ. Уровень сигнала от минус 15 до минус 5 дБ.
- «Сигнал вмешательства» информирует абонентов УПАТС, участвующих в разговоре, о подключении оператора или третьего абонента. Прерывистый синусоидальный сигнал частотой 425 ± 3 Гц, первый импульс 0,25 ± 0,025 с, первая пауза 0,25 ± 0,025 с, второй импульс 0,25 ± 0,025 с, вторая пауза 1,25 ± 0,3 с. Сигнал передается в течение всего времени вмешательства на фоне разговора. Уровень сигнала от минус 20 до минус 10 дБ. Сигнал используется для предоставления абонентам дополнительных услуг.
- «Сигнал уведомления» информирует абонента, занятого в разговоре, о поступлении нового вызова. Прерывистый синусоидальный сигнал частотой 425 ± 3 Гц, импульс 0,2 ± 0,02 с, пауза 5,0 ± 0,5 с. Уровень сигнала от минус 20 до минус 10 дБ. Сигнал используется для предоставления абонентам дополнительных услуг.
- «Сигнал отключения участника конференц-связи» информирует абонентов, участвующих в конференц-связи, об отключении одного из участников. Сигнал

отключения — одиночный синусоидальный импульс частотой 425 ± 3 Гц, продолжительностью 0,3–1,0 с. Изменение уровня от минус 15 до минус 5 дБ.

- «Сигнал неполного сбора» информирует абонента-инициатора о том, что врем сбора конференц-связи окончилось, но подключились не все абоненты. Одиночный синусоидальный сигнал частотой 425 ± 3 Гц продолжительностью 0,3–1,0 с. Изменение уровня от минус 5 до минус 15 дБ.
- «Подтверждение приема» информирует абонента о том, что заказ на услугу принят или произведена отмена услуги. При положительном исходе абоненту передается сигнал «Ответ станции», при отрицательном — «Указательный сигнал».
- «Ожидание» (контроль посылки сигнала уведомления) — информирует вызывающего абонента о посылке вызываемому абоненту сигнала «уведомление». Прерывистый синусоидальный сигнал частотой 425 ± 3 Гц, посылка 0,2 ± 0,02 с, пауза 5 ± 0,5 с. Уровень сигнала в точке с нулевым относительным уровнем от минус 15 до минус 5 дБ.

Станция должна обеспечивать прием акустических сигналов частоты 425 Гц, поступающих от встречных станций (АРМ-20 и АТС-ДШ), с помощью приемника акустических сигналов.

Приемник акустических сигналов должен удовлетворять следующим требованиям:

- условия гарантированного срабатывания:
- диапазон частот 425± 30 Гц;
- диапазон уровней минус 4,3 — минус 28,0 дБ;
- время распознавания 150 ± 2 мс;
- условия гарантированного несрабатывания:
- отклонение частоты входных сигналов более ± 50 Гц от номинального значения 425 Гц;
- длительность сигнала 100 мс и менее;
- уровень несрабатывания минус 34 дБ.

Условия защиты от помех:

- приемник не должен реагировать на перерывы, длительностью 5 мс и менее; прекращение сигнала на время больше 100 мс должно восприниматься приемником как сигнал окончания распознавания;
- коэффициент нелинейных искажений акустических сигналов должен быть не более 5%;
- должна обеспечиваться возможность введения новых акустических сигналов по мере расширения перечня предоставляемых услуг.

Эксплуатация и ремонт абонентских устройств городских телефонных сетей

Связь между абонентскими устройствами осуществляется с помощью узлов коммутации, в которых информация концентрируется и затем направляется по определенным путям. Для этого узлы коммутации соединяются между собой линейными сооружениями (соединительными линиями), в которые входят системы каналообразующего оборудования, организующие необходимые пучки каналов по кабельным, радиорелейным и спутниковым линиям связи.

Совокупность узлов коммутации, оконечных абонентских устройств и соединяющих их каналов и линий связи называют сетью телефонной связи.

Телефонная связь является одним из видов электрической связи. Для совершенствования системы электрической связи в стране ведется большая работа по созданию Единой автоматизированной сети связи (ЕАСС). Сеть ЕАСС предназначена для передачи различных видов информации: телефонных и телеграфных сообщений программ звукового вещания и телевидения, передачи газет, данных и фототелеграмм.

Для качественной передачи различных видов информации организуют стандартные (типовые) каналы, которые характеризуются определенными параметрами. Одним из таких параметров является ширина эффективно передаваемой полосы частот, составляющая 300–3400 Гц для передачи телефонных сообщений. Для передачи программ телевидения, газет, высокоскоростной передачи данных необходимы каналы с более широкой полосой частот-групповые тракты. Типовые каналы передачи и групповые тракты составляют первичную сеть, которая является основой ЕАСС и охватывает всю территорию СССР; из типовых кана-

лов и групповых трактов первичной сети создаются вторичные сети ЕАСС.

Классификация телефонных сетей. Сети связи создаются для передачи информации между абонентами и бывают коммутируемыми и некоммутируемыми. Сеть называется коммутируемой, когда тракт передачи информации создается по запросу абонента на время передачи сообщения, и некоммутируемой, когда тракт передачи информации обеспечивается постоянным соединением между определенными абонентами и нет необходимости в коммутации. Телефонные сети являются коммутируемыми. Общегосударственная телефонная сеть состоит из междугородной телефонной сети и зоновых телефонных сетей. Междугородная телефонная сеть обеспечивает соединение автоматических междугородных телефонных станций (АМТС) различных зон.

Зоновая телефонная сеть состоит из местных телефонных сетей, расположенных на территории зоны и внутризоновой телефонной сети. Местные телефонные сети разделяются на городские, обслуживающие город и ближайшие пригороды (ГТС), и сельские (СТС), обеспечивающие связь в пределах сельского административного района.

Учрежденческо-производственная телефонная сеть (УПТС) служит для внутренней связи предприятий, учреждений, организаций и может быть соединена с сетью общего пользования либо быть автономной.

Построение телефонных сетей. Зоновая телефонная сеть включает всех абонентов определенной территории, охватываемой единой семизначной нумерацией, и является частью ОАКТС. Территории зоновых сетей совпадают с территориями административных областей (республик). В зависимости от конфигурации области и телефонной плотности территории нескольких областей могут быть объединены в одну зону и, наоборот, одна область может быть разделена на две зоны и более. Зоновая сеть включает в себя ГТС и СТС, причем на территории одной зоны может быть несколько ГТС и СТС. Крупные города с семизначной нумерацией выделяются в самостоятельные зоны.

Сельские телефонные сети охватывают более обширные территории, чем городские, но плотность телефонных аппаратов значительно меньше. Поэтому емкость автоматических телефонных станции АТС в сельских местностях значительно меньше, чем в городах.

В районном центре сельской местности устанавливается центральная станция (ЦС), которая является коммутационным узлом и выполняет одновременно функции городской телефонной станции районного центра. Из-за большой территории СТС и малой плотности телефонных аппаратов непосредственное включение всех абонентских

линий в ЦС экономически не оправдано. Поэтому на СТС применяют узлообразование с различной степенью децентрализации станционного оборудования.

В настоящее время используют одно- и двухступенчатое построение СТС.

При одноступенчатом построении СТС кроме ЦС имеются оконечные телефонные станции ОС, включаемые непосредственно в ЦС районного центра. В этом случае в соединении между сельскими абонентами двух различных ОС участвует только один узел автоматической коммутации — станции ЦС.

На СТС, занимающих большую территорию из экономических соображений, применяют двухступенчатое построение с различными коммутационными узлами. В этом случае на СТС устанавливают ЦС, ОС и узловые станции (УС). Наибольшее количество станций, через которые могут соединяться абоненты на СТС, достигает пяти (ОС — УС — ЦС — УС — ОС).

Зоновые сети имеют оконечные АМТС, входящие в междугородную телефонную сеть. Через АМТС междугородная сеть объединяет все зоновые сети в единую ОАКТС. Городская и сельская телефонные сети связаны с АМТС своей зоны. Если в зоне несколько таких АМТС, одна из них является основной, причем АМТС одной зоны связываются между собой каналами по принципу «каждая с каждой». С АМТС зоны непосредственно соединяются районные АТС (РАТС) или междугородные узлы входящего сообщения городских телефонных сетей (УВСМ).

Для объединения зоновых телефонных сетей страны в общегосударственную создается междугородная телефонная сеть, в которую входят узлы автоматической коммутации первого класса (УАК-1) и второго класса (УАК-Н).

Все узлы автоматической коммутации УАК-1 соединяются между собой по принципу «каждый с каждым», обслуживают определенные территориальные районы и являются центром сети радиально-узлового построения. Узлы автоматической коммутации УАК-1 объединяют УАК-11 и АМТС. Все АМТС, расположенные на зоновых сетях, являются оконечными станциями междугородной сети, а УАК-транзитными. При большой нагрузке между АМТС устанавливается непосредственная связь.

Городская телефонная сеть состоит из комплекса сооружений (станционное оборудование, здание, линейные сооружения, абонентские устройства и др.), обеспечивающих телефонной связью абонентов

города и прилегающих к нему пригородов. Стоимость линейных сооружений в значительной степени зависит от принципа построения ГТС и ее емкости.

По принципу построения ГТС делятся на нерайонированные и районированные. Районированные телефонные сети, в свою очередь, подразделяются на ГТС без узлов, ГТС с узлами входящего сообщения (УВС), а также с узлами исходящего (УИС) и входящего сообщений.

Простейшей является нерайонированная телефонная сеть, имеющая одну АТС, линейные сооружения которой состоят только из абонентских линий.

На нерайонированной сети могут быть соединительные линии (СЛ, СЛМ, ЗСЛ), необходимые для связи АТС с учрежденческо-производственной телефонной станцией УПАТС и междугородной телефонной станцией АМТС.

Структурная схема нерайонированной ГТС небольшого города следующая. К городской автоматической телефонной станции (ГАТС) подключены индивидуальные абонентские линии, абонентские линии со спаренными телефонными аппаратами и линии таксофонов. Одновременно ГАТС связана односторонними соединительными линиями с АМТС и УПАТС. К АМТС подключены междугородные каналы и переговорные пункты: центральный (ЦПП) и районный (РПП). Кроме того, ГАТС выполняет роль связующего звена между УПАТС и АМТС, не имеющими непосредственной связи между собой.

Емкость нерайонированных телефонных сетей не превышает обычно 8000 номеров. Такие телефонные сети строятся в большинстве районных центров нашей страны.

С увеличением емкости ГТС нерайонированная сеть оказывается неэкономичной из-за большой протяженности абонентских линий, (эксплуатация которых высока, а использование мало), а также высокой стоимости строительства. Повышение использования линейных сооружений может быть достигнуто районированием (децентрализацией станционного оборудования), которое рекомендуется производить, начиная с емкости 10000 номеров.

При емкости ГТС от 10 000 до 50 000 номеров территория города делится на районы, обслуживаемые районными АТС (РАТС). Протяженность абонентских линии на районированной ГТС сокращается, так как АТС приближается к местам установки телефонных аппаратов. Районные АТС соединяют между собой линиями (СЛ) по принципу «каждая с каждой», при этом достигается более высокое использование пучков

СЛ. Так как телефонное сообщение, возникающее на каждой РАТС, распределяется по небольшому числу направлений, пучки СЛ между РАТС получаются крупными.

Нумерация абонентских линий на таких ГТС пятизначная, первая цифра номера является кодом РАТС. С увеличением емкости районированной ГТС растет число РАТС, а следовательно, число пучков СЛ, что уменьшает их использование. При большом числе РАТС связь их по принципу «каждая с каждой» становится экономически нецелесообразной.

При емкости ГТС от 50 000 до 500 000 номеров сеть наиболее экономично строить с УВС. При таком построении ГТС делится на узловые районы, в каждом из которых может быть установлено несколько РАТС, соединяющихся между собой по принципу «каждая с каждой». Связь между РАТС одного узлового района может осуществляться через УВС. Для соединения между собой абонентов разных узловых районов в каждом из них устанавливается УВС.

Каждая РАТС телефонной сети соединяется с УВС других узловых районов сети исходящими, а со своим УВС — входящими СЛ. При наличии УВС на ГТС пучки СЛ от РАТС к УВС других узловых районов и от УВС к своим РАТС укрупняются. На районированных ГТС с УВС применяют шестизначную нумерацию, первая цифра является кодом узлового района, а вторая — кодом РАТС.

В настоящее время многие ГТС СССР построены с УВС. С ростом числа РАТС эффект узлообразования возрастает. При емкости ГТС более 500 000 номеров даже при наличии на сети УВС число пучков СЛ становится очень большим, емкость и использование их уменьшаются. В этом случае использование СЛ увеличивают образованием на районированной телефонной сети, кроме УВС — УИС. Территория города делится на миллионные зоны, каждая из которых может включать в себя до десяти узловых районов емкостью до 100 000 номеров каждый. Концентрируемая на УИС исходящая телефонная нагрузка по крупным пучкам СЛ поступает к УВС других узловых районов. Число и протяженность пучков СЛ значительно уменьшаются, а использование их возрастает.

В пределах узлового района РАТС соединяются между собой по принципу «каждая с каждой», а с РАТС других узловых районов — через УИС и УВС.

На ГТС с УИС и УВС применяют семизначную нумерацию; первая цифра номера определяет код миллионной зоны, вторая — код узлового района, а третья — код РАТС.

Связи между РАТС одного узлового района осуществляются по принципу «каждая с каждой» либо через УВС.

Абонентские линии являются линиями двустороннего действия, т.е. по этой линии абонент вызывает станцию и станцию абонента. Соединительные линии между РАТС являются линиями одностороннего действия, поэтому для каждой РАТС необходимы два вида пучков СЛ — один для исходящей связи, второй — для входящей.

Для обслуживания телефонной связью крупных промышленных предприятий, учреждений, больниц, гостиниц в них организуется своя телефонная сеть, обслуживаема самостоятельной учрежденческо-производственной АТС (УПАТС). Какой-то части абонентов предоставляется возможность связи с абонентами городской телефонной сети. Для этого между УПАТС и ближайшей РАТС прокладывают соединительные линии, которые являются линиями одностороннего действия, при этом название линий — исходящие и входящие — принимаются относительно УПАТС. При исходящей связи абонент УПАТС набирает индекс выхода (цифра 9 или 0) на РАТС, после чего он может набрать номер любого абонента городской телефонной сети. Нумерация абонентов УПАТС может быть двух-, трех или четырехзначная в зависимости от емкости УПАТС. При полноавтоматической входящей связи с абонентами УПАТС нумерация абонентов входит в нумерацию городской телефонной сети.

Под системой нумерации понимают определенную комбинацию цифр, характеризующую телефонный адрес вызываемого абонента и передаваемую на телефонную станцию абонентом.

Общегосударственная автоматически коммутируемая телефонная сеть должна обеспечивать минимальную значность номера и неизменность системы нумерации в течение длительного периода (до 50 лет).

Нумерация может быть закрытой и открытой. Нумерация называется закрытой (единой), если абонент вызывается набором одного и того же номера независимо от места нахождения вызывающего пункта. При закрытой системе нумерации номер вызывающего абонента не зависит от вида связи — местной, зоновой или междугородной. Нумерация называется открытой, если зависит от вида связи: местной, зоновой или междугородной.

В ОАКТС принята открытая система нумерации с постоянными кодами. Междугородный номер абонента на сети страны содержит десять цифр и имеет структуру АВСабхххxx, где АВС — постоянный трехзначный код зоны, аб — код местной сети или стотысячной группы абонентов, а последние пять цифр ххххх — пятизначный номер абонента.

В соответствии с принятым в СССР зоновым принципом нумерации вся территория страны разделена на 166 телефонных зон с единой семизначной нумерацией абонентов.

При автоматической междугородной связи абонент в первую очередь набирает установленный (единый в СССР) индекс выхода на АМТС — цифру 8, а затем код зоны АВС и после этого семь цифр зонового абонентского номера. При вызове абонентов ГТС областного центра с пятизначной или шестизначной местной нумерацией местный номер абонента должен дополняться до зонового (семизначного) соответственно цифрами 22 или 2. При вызове абонентов ГТС областного центра, где не организована зона (нет АМТС), временно допускается дополнять нулями местный номер абонента до зонового. Например, при вызове абонента г. Нальчика необходимо набрать: 8 866 00 2 48 26.

В качестве А могут быть использованы все цифры, кроме 1 и 2, а в качестве В и С — любые цифры. Первая цифра абонентского номера не может быть 8 и 0 при семи-шести-пятизначной нумерации.

При внутризоновой связи вместо АВС набирается цифра 2 (т. е. 82 аб ххххх), которая является внутризоновым кодом. В качестве а могут быть использованы цифры кроме 8 и 0, а в качестве б — любые цифры.

На ГТС нашей страны, как правило, применяют закрытую систему нумерации. Число знаков в номере абонента зависит только от емкости ГТС. Если на ГТС принята семизначная нумерация, то местный и зоновый номера совпадают (например, ГТС Москвы, Ленинграда, Киева). При автоматической международной телефонной связи абонент должен набрать: цифры 8, 10, международный номер (где 10 — индекс выхода на автоматическую международную телефонную сеть). Полный международный номер вызываемого абонента может иметь 11—12 знаков.

Абонентские и соединительные линии и повышение их использования. Абонентские линии представляют собой наименее используемую часть сооружений ГТС, а затраты на них составляют около 30% общих затрат на линейные сооружения. Поэтому необходимы способы повышения использования этих индивидуальных линий. Наибольшее распространение получило спаренное включение двух телефонных аппаратов в одну абонентскую линию. При этом каждый из аппаратов имеет самостоятельный номер. Для спаренного включения ранее применяли релейные блокираторы. В настоящее время используют диодно-транзисторные приставки, смонтированные непосредственно в телефонной розетке.

К недостаткам спаренного включения относятся: невозможность одновременного ведения разговора, перехват вызова одного абонента

другим, если последний снимает микротелефонную трубку первым, сложность предоставления междугородных переговоров, невозможность связи между спаренными телефонными аппаратами.

В настоящее время для коллективного включения двух аппаратов в одну абонентскую линию применяют абонентскую высокочастотную установку (АВУ). В данном случае разделение цепей происходит по частоте, поэтому при включении двух аппаратов с АВУ оба абонента могут пользоваться связью одновременно, а не поочередно.

Во избежание усложнения абонентской проводки спаренное включение допускается только для телефонных аппаратов квартирного сектора, расположенных в непосредственной близости один от другого.

Экономического эффекта от широкого применения спаренного включения аппаратов на ГТС достигают только при большой протяженности абонентских линий. С увеличением телефонной плотности ГТС длина абонентских линий сокращается и, следовательно, экономическая целесообразность спаренного включения уменьшается. Однако на нерайонированный ГТС, а также при большой протяженности абонентских линий спаренное включение будет применяться еще длительное время (например, на СТС).

Снижение затрат на абонентские линии достигается использованием телефонных подстанций на ГТС, которые следует рассматривать как децентрализацию коммутационного оборудования, т. е. приближение части РАТС к месту установки телефонных аппаратов. Подстанции представляют собой часть оборудования РАТС, установленного в отдельном помещении вблизи места сосредоточения аппаратов абонентов. Подстанция с «опорной» РАТС соединяется пучком исходящих и двум пучками входящих СЛ (для местной и междугородной связи), число которых значительно меньше числа абонентских линий. Нумерация абонентов подстанции входит в нумерацию «опорной» РАТС.

Применение подстанций значительно снижает затраты на магистральные кабели абонентской сети. В настоящее время на телефонных сетях широко применяют подстанции ПСК-1000.

Межстанционные соединительные линии являются важнейшей частью тракта на ГТС. На районированных ГТС, особенно в крупных городах, расход кабеля на межстанционные связи может превышать расход кабеля на абонентские линии. Поэтому большое значение имеет увеличение использования СЛ. Одним из способов такого увеличения является укрупнение пучков линий рациональным построением ГТС — узлообразованием. Другой способ — применение различных систем передачи — аппаратуры высокочастотного телефонирования КРР «КАМА», позво-

ляющей по одной паре кабеля передавать одновременно 30 телефонных разговоров, и аппаратуры с импульсно-кодовой модуляцией ИКМ-30.

В настоящее время разработаны новые принципы построения телефонных сетей, в основу которых положено объединение систем передачи и коммутации на основе импульсно-кодовой модуляции. Такое построение телефонных сетей называется единой системой «уплотнение — коммутация», а ГТС, построенные по этому принципу, называются интегральными телефонными сетями.

Как осуществляется выход на междугородку

Каждому абоненту городской телефонной сети должна быть обеспечена связь не только с абонентами своей телефонной сети, но и с абонентами любой другой сети страны. Для этого между РАТС и МТС прокладывают соединительные линии, назначение и способ включения которых зависят от типа МТС (РМТС или АМТС) города. Организация связи ГТС и МТС зависит от способа установления междугородных соединений. Широко используют ручной и полуавтоматический способы установления соединений. В последнее время на междугородной телефонной сети интенсивно внедряют автоматический способ. В соответствии с этим во всех городах страны, в которых имеются РМТС, устанавливается в основном аппаратура АМТС. Связь между ГАТС и РМТС осуществляется по двум видам линий: заказным и соединительным.

Заказные линии используют только для передачи заказов на междугородные переговоры от абонентов ГТС. На МТС заказные линии включают в специальные заказные и междугородные коммутаторы.

Соединительные линии предназначены для связи МТС с РАТС. При наличии в городе АМТС она связывается с РАТС двумя пучками линий: заказно-соединительных и соединительных междугородных. Заказно-соединительные линии (исходящие) предназначены для осуществления исходящих междугородных соединений через АМТС. На ГТС заказно-соединительные линии включены в восьмую декаду 1ГИ и оборудуются исходящими комплектами заказно-соединительных линий ИКЗСЛ, промежуточными регистрами ПР и устройством запроса и приема информации УЗПИ.

При автоматическом способе установления междугородного соединения необходимо передать на АМТС информацию о номере вызывающего абонента. Для этого разработана и широко внедряется на городских телефонных сетях аппаратура автоматического определения

категории и номера вызывающего абонента АОН, которая является передающей частью УЗПИ. Информация из АОН передается через УЗПИ в ПР. В дальнейшем информация из АОН будет передаваться непосредственно в АМТС и тогда установка ПР и УЗПИ на РАТС не потребуется.

В качестве индекса выхода на АМТС по заказно-соединительным линиям для Советского Союза принята цифра 8. Соединительные линии междугородной связи предназначены для осуществления входящих междугородных соединений с абонентами ГТС через соответствующие АТС.

При внедрении на междугородной сети автоматического способа соединений, когда абонент, набирая номер, управляет установлением соединения, от местной сети и исходящей АМТС требуется учитывать каждый состоявшийся междугородный разговор с последующим оформлением счета для оплаты. Для предъявления счета абоненту, необходимо определить стоимость разговора и убедиться, что разговаривал именно этот абонент.

На междугородной сети принят Централизованный учет стоимости междугородных разговоров. В состав АМТС входит специальная аппаратура, которая выдает необходимую информацию о каждом состоявшемся разговоре на перфокарту, перфоленту или магнитную ленту. На машинно-счетной станции или в вычислительном центре эта информация обрабатывается и печатается в виде счетов, которые предъявляют абонентам к оплате.

Автоматизация процесса соединения телефонных аппаратов

На ручных телефонных станциях операции, необходимые для соединения абонентских линий, распределены между абонентами и телефонисткой. Абонент автоматической телефонной станции выполняет, по существу, те же функции, что и абонент РТС. Он посылает сигнал вызова на станцию снятием микротелефонной трубки, а сигнал отбоя — опусканием микротелефонной трубки на рычажный переключатель телефонного аппарата. Но информация о номере вызываемого абонента передается по-иному, т. е. абонент АТС с помощью номеронабирателя набирает цифры нужного номера, в результате чего посылаются импульсы постоянного тока, которые будут управлять работой механизмов АТС.

На городских телефонных сетях работают АТС декадно-шаговой (АТС-47 и АТС-54), а также координатной (АТСК, АТСКУ, ARF-50 и Пентаконта) систем.

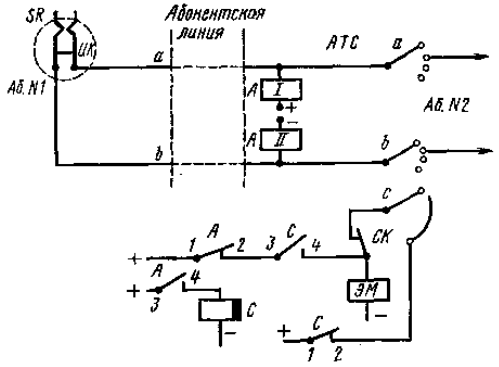
Элементами автоматизации являются реле, искатели и полупроводниковые приборы, с помощью которых осуществляется соединение между линиями абонентов АТС. Эти элементы управляются импульсами постоянного тока, которые создаются номеронабирателем телефонного аппарата при наборе абонентом цифр номера вызываемого абонента.

Простейший искатель состоит из электромагнита, снабженного якорем, храпового колеса, щеток, укрепленных на одной оси с храповиком, и контактного поля с ламелями. Количество щеток и емкость контактного поля искателя могут быть различными в зависимости от его назначения.

В состоянии покоя якорь удерживается пружиной. При нажатии ключа через обмотку электромагнита пройдет ток, его сердечник намагнитится и притянет якорь. При этом собачка повернет храповое колесо на один шаг и контактные щетки перейдут с исходной ламели на первую. Если теперь разомкнуть цепь тока через обмотку электромагнита, то под действием пружины якорь вернется в исходное положение, а собачка, скользя по скосу зуба, западет на следующий зуб. При повторном замыкании цепи ключом якорь вновь притянется, щетки перейдут с первой контактной ламели на вторую и т. д.

Таким образом создается возможность установить щетки искателя на одной из его ламелей. Это и используют на АТС для соединения абонентских линий.

Ниже изображена схема, поясняющая принцип соединения абонентских линий на АТС (в данном случае нумерация абонентских линий однозначная). Номеронабиратель телефонного аппарата абонента № 1 изображен в виде замкнутого импульсного контакта ИК.



Линия абонента № 1 на станции включена в абонентское реле, через обмотки которого осуществляется питание микрофона аппарата абонента, а контакты используются для управления процессом соединения. Когда абонент № 1 снимает микротелефонную трубку с рычага аппарата, замыкается цепь для работы реле А: плюс ЦБ, обмотка / реле А, провод а, импульсный контакт ИК номеронабирателя SR, провод b, обмотка // реле А, минус батареи.

Реле А притягивает якорь, вследствие чего его контакты 1–2 размыкаются, а контакты 3–4 замыкаются. При этом создается цепь для срабатывания реле С: плюс, контакты 3–4 реле Л, обмотка реле С, минус. Это реле замедленного действия на отпускание, поэтому, когда ток не проходит через его обмотку в течение 0,1 с, якорь его останется в притянутом состоянии.

При срабатывании реле С размыкаются его контакты /-Ч и замыкаются контакты 3–4, однако ток через обмотку электромагнита ЭМ искателя пройти не может, так как цепь разомкнута контактами 1–2 реле А.

При наборе абонентом номера вызываемого телефонного аппарата цепь тока через обмотку реле А прерывается контактом ИК номеронабирателя. В течение времени размыкания цепи контакты 1–2 и 3–4 реле А принимают положение покоя (так, как изображено на схеме). При отпускании якоря реле А цепь тока через обмотку реле С хотя и обрывается, но якорь не отпускает, так как время обрыва цепи меньше времени отпускания этого реле.

Когда якорь реле А отпущен, а якорь реле С притянут, создается цепь прохождения тока через электромагнит ЭМ: плюс, контакты /-2 реле А, контакты 3–4 реле С, обмотка электромагнита ЭМ, минус. Поэтому каждое отпускание якоря реле Л сопровождается притяжением якоря электромагнита ЭМ искателя и, следовательно, передвижением щеток а, b и с на один шаг.

При наборе абонентом, например цифры 2, щетки искателя останавливаются на втором контакте (ламеле) и соединяют линию вызывающего абонента с линией вызываемого абонента (в данном случае со второй).

Когда по окончании разговора абоненты положат микротелефонные трубки на аппарат, реле А лишится тока и отпустит якорь. Так как при этом разомкнутся его контакты 3–4, то спустя некоторое время (около 0,1 с) отпустит якорь реле С, искатель начнет возвращаться в исходное положение, получая ток для работы по цепи: плюс, контакты 1–2 реле С, сплошная ламель искателя, щетка с, самопрерывающийся контакт С/С, обмотка электромагнита ЭМ, минус.

При каждом притяжении якоря электромагнита ЭМ контакт СК прерывается и обрывает цепь тока через обмотку электромагнита ЭМ, последний отпускает якорь и вновь притягивает его, так как контакт С/С замыкается.

Работа электромагнита продолжается до тех пор, пока щетка с не займет исходное положение и через обмотку электромагнита перестанет проходить ток.

Четкость работы реле и электромагнитов искателей в большой степени зависит от времени размыкания импульсного контакта ИК номеронабирателя телефонного аппарата. Если время размыканий этого контакта будет больше 0,1 с, то при размыкании контактов 3–4 реле А реле С не сможет удержать якорь и соединения не произойдет.

При большой частоте импульсов и малой их длительности электромагнит ЭМ может не успеть притянуть свой якорь и тогда соединение также не произойдет. Именно поэтому к номеронабирателю телефонных аппаратов предъявляют жесткие требования, а именно: частота создаваемых импульсов должна находиться в пределах (10 ± 1) имп/с; отношение времени размыкания к времени замыкания импульсных контактов (импульсный коэффициент) не должно выходить за пределы 1,4–1,8.

Вводные устройства телефонной сети

Кабельные боксы. Бокс БКТ представляет собой чугунную коробку со съемной задней крышкой.

На лицевой стенке бокса прорезаны окна, в которых укреплены пластмассовые колодки со сквозными клеммами, называемые плинтами. С наружной стороны плинта сквозная клемма имеет винт для присоединения проводника, а с внутренней — металлическую луженую пластинку с отверстием (перо), к которой припаивают жилу кабеля. В нижней части бокса сделано отверстие с запрессованной луженой стальной втулкой, через которую конец кабеля вводят внутрь бокса и закрепляют его во втулке. Каждая колодка снабжена 20 клеммами, расположенными в два ряда, для включения 10 пар жил.

Боксы выпускают емкостью 100 Х 2, 50 Х 2, 30 Х 2 и 20 Х 2. Соответственно на них установлено 10, 5, 3 и 2 плинта. Нумерация плинтов на боксах и пар на плинтах начинается с нуля.

Боксы устанавливают обычно в помещении или в специальных шкафах, называемых распределительными. Корпус бокса снабжен лапками для укрепления его болтами на каркасе распределительного шкафа.

Распределительные коробки 10 Х 2. Распределительная коробка КРТ-10 состоит из чугунного корпуса и откидной крышки. Внутри корпуса укреплен бокс 10 Х 2 с одним плинтом. Кабели, введенные в различные здания, распаивают в перчатках на десятипарные и включают их в распределительные коробки, устанавливаемые на лестничных клетках и в коридорах. Распределительные коробки крепят к стенке за лапки двумя шурупами.

Кроме распределительных коробок КРТ-10 промышленность выпускает распределительные коробки КРТП в пластмассовом корпусе наклонного типа.

Кабельные ящики. Кабельный ящик по существу является боксом. Его устанавливают непосредственно на кабельных опорах или на чердаках зданий при переходе кабельной линии в воздушную. На плинте кабельного ящика укреплены предохранители и угольные разрядники, защищающие кабель от опасных напряжений и сильных токов, которые могут возникнуть в проводах воздушной линии. Кроме того, плинт закрыт металлической крышкой, которая защищает его от атмосферных осадков и механических повреждений. Для вывода из-под крышки изолированных проводников, присоединяемых к проводам воздушной линии, в основании сделано два специальных отверстия. Кабельные ящики крепят к столбу или доске за лапки двум шурупами.

На ГТС применяются кабельные ящики двух типов: ЯКГ-10-2 для включения десяти пар проводов с одним десятипарным плинтом и ЯКГ-20-2 для включения 20 пар проводов с двумя плинтами.

Современная электрическая связь

Краткий обзор развития линий связи

Линии связи возникли одновременно с появлением электрического телеграфа. Первые линии связи были кабельными. Однако вследствие несовершенства конструкции кабелей подземные кабельные линии связи вскоре уступили место воздушным. Первая воздушная линия большой протяженности была построена в 1854 г. между Петербургом и Варшавой. В начале 70-х годов прошлого столетия была построена воздушная телеграфная линия от Петербурга до Владивостока длиной около 10 тыс. км. В 1939 г. была пущена в эксплуатацию величайшая в мире по протяженности высокочастотная телефонная магистраль Москва—Хабаровск длиной 8300 км.

Создание первых кабельных линий связано с именем русского ученого П. Л. Шиллинга. Еще в 1812 г. Шиллинг в Петербурге демонстрировал взрывы морских мин, использовав для этой цели созданный им изолированный проводник.

В 1851 г. одновременно с постройкой железной дороги между Москвой и Петербургом был проложен телеграфный кабель, изолированный гуттаперчей. Первые подводные кабели были проложены в 1852 г. через Северную Двину и в 1879 г. через Каспийское море между Баку и Красноводском. В 1866 г. вступила в строй кабельная трансатлантическая магистраль телеграфной связи между Францией и США.

В 1882—1884 гг. в Москве, Петрограде, Риге, Одессе были построены первые в России городские телефонные сети. В 90-х годах прошлого столетия на городских телефонных сетях Москвы и Петрограда были подвешены первые кабели, насчитывающие до 54 жил. В 1901 г. началась постройка подземной городской телефонной сети.

Первые конструкции кабелей связи, относящиеся к началу XX века, позволили осуществлять телефонную передачу на небольшие расстояния. Это были так называемые городские телефонные кабели с воздушно-бумажной изоляцией жил и парной их скруткой. В 1900—1902 гг. была сделана успешная попытка повысить дальность передачи методами искусственного увеличения индуктивности кабелей путем включения в цепь катушек индуктивности (предложение Пупина), а также применения токопроводящих жил с ферромагнитной обмоткой (предложение Крарупа). Такие способы на том этапе позволили увеличить дальность телеграфной и телефонной связи в несколько раз.

Важным этапом в развитии техники связи явилось изобретение, а начиная с 1912—1913 гг. освоение производства электронных ламп. В 1917 г. В. И. Коваленковым был разработан и испытан на линии телефонный усилитель на электронных лампах. В 1923 г. была осуществлена телефонная связь с усилителями на линии Харьков—Москва—Петроград.

В 30-х годах началось развитие многоканальных систем передачи. В последующем стремление расширить спектр передаваемых частот и увеличить пропускную способность линий привело к созданию новых типов кабелей, так называемых коаксиальных. Но массовое изготовление их относится лишь к 1935 г., к моменту появления новых высококачественных диэлектриков типа эскапона, высокочастотной керамики, полистирола, стирофлекса и т. д. Эти кабели допускают передачу энергии при частоте токов до нескольких миллионов герц и позволяют производить по ним передачу телевизионных программ на большие расстояния. Первая коаксиальная линия на 240 каналов ВЧ телефонирования была проложена в 1936 г. По первым трансатлантическим подводным кабелям, проложенным в 1856 г., организовывали лишь телеграфную связь,

и только через 100 лет, в 1956 г., была сооружена подводная коаксиальная магистраль между Европой и Америкой для многоканальной телефонной связи.

В 1965—1967 гг. появились опытные волноводные линии связи для передачи широкополосной информации, а также криогенные сверхпроводящие кабельные линии с весьма малым затуханием. С 1970 г. активно развернулись работы по созданию световодов и оптических кабелей, использующих видимое и инфракрасное излучения оптического диапазона волн.

Создание волоконного световода и получение непрерывной генерации полупроводникового лазера сыграли решающую роль в быстром развитии волоконно-оптической связи. К началу 80-х годов были разработаны и испытаны в реальных условиях волоконно-оптические системы связи. Основные сферы применения таких систем — телефонная сеть, кабельное телевидение, внутриобъектовая связь, вычислительная техника, система контроля и управления технологическими процессами и т. д.

В России и других странах проложены городские и междугородные волоконно-оптические линии связи. Им отводится ведущее место в научно-техническом прогрессе отрасли связи.

Линии связи и основные свойства ВОЛС

На современном этапе развития общества в условиях научно-технического прогресса непрерывно возрастает объем информации. Как показывают теоретические и экспериментальные (статистические) исследования, продукция отрасли связи, выражающаяся в объеме передаваемой информации, возрастает пропорционально квадрату прироста валового продукта народного хозяйства. Это определяется необходимостью расширения взаимосвязи между различными звеньями народного хозяйства, а также увеличением объема информации в технической, научной, политической и культурной жизни общества. Повышаются требования к скорости и качеству передачи разнообразной информации, увеличиваются расстояния между абонентами. Связь необходима для оперативного управления экономикой и работы государственных органов, для повышения обороноспособности страны и удовлетворения культурно-бытовых потребностей населения.

В эпоху научно-технической революции связь стала составным звеном производственного процесса. Она используется для управления технологическими процессами, электронно-вычислительными машинами, роботами, промышленными предприятиями т.д. Непременным и одним из наиболее сложных и дорогостоящих элементов связи являются

линии связи (ЛС), по которым передаются информационные электромагнитные сигналы от одного абонента (станции, передатчика, регенератора и т.д.) к другому (станции, регенератору, приемнику и т.д.) и обратно. Очевидно, что эффективность работы систем связи во многом предопределяется качеством ЛС, их свойствами и параметрами, а также зависимостью этих величин от частоты и воздействия различных факторов, включая мешающие влияния сторонних электромагнитных полей.

Различают два основных типа ЛС: линии в атмосфере (радиолинии РЛ) и направляющие линии передачи (линии связи).

Отличительной особенностью направляющих линий связи является то, что распространение сигналов в них от одного абонента (станции, устройства, элемента схемы и т.д.) к другому осуществляется только по специально созданным цепям и трактам ЛС, образующим направляющие системы, предназначенные для передачи электромагнитных сигналов в заданном направлении с должными качеством и надежностью.

В настоящее время по линиям связи передаются сигналы от постоянного тока до оптического диапазона частот, а рабочий диапазон длин волн простирается от 0,85 мкм до сотен километров.

Различают три основных типа ЛС: кабельные (КЛ), воздушные (ВЛ), волоконно-оптические (ВОЛС). Кабельные и воздушные линии относятся к проводным линиям, у которых направляющие системы образуются системами «проводник—диэлектрик», а волоконно-оптические линии представляют собой диэлектрические волноводы, направляющая система которых состоит из диэлектриков с различными показателями преломления.

Волоконно-оптические линии связи представляют собой системы для передачи световых сигналов микроволнового диапазона волн от 0,8 до 1,6 мкм по оптическим кабелям. Этот вид линий связи рассматривается как наиболее перспективный. Достоинствами ВОЛС являются низкие потери, большая пропускная способность, малые масса и габаритные размеры, экономия цветных металлов, высокая степень защищенности от внешних и взаимных помех.

Основные требования к линиям связи

В общем виде требования, предъявляемые высокоразвитой современной техникой электросвязи к междугородным линиям связи, могут быть сформулированы следующим образом:

- осуществление связи на расстояния до 12500 км в пределах страны и до 25 000 для международной связи;

- широкополосность и пригодность для передачи различных видов современной информации (телевидение, телефонирование, передача данных, вещание, передача полос газет и т. д.);
- защищенность цепей от взаимных и внешних помех, а также от грозы и коррозии;
- стабильность электрических параметров линии, устойчивость и надежность связи;
- экономичность системы связи в целом.

Кабельная линия междугородной связи представляет собой сложное техническое сооружение, состоящее из огромного числа элементов. Так как линия предназначена для длительной работы (десятки лет) и на ней должна быть обеспечена бесперебойная работа сотен и тысяч каналов связи, то ко всем элементам линейно-кабельного оборудования, и в первую очередь к кабелям и кабельной арматуре, входящим в линейный тракт передачи сигналов, предъявляются высокие требования. Выбор типа и конструкции линии связи определяется не только процессом распространения энергии вдоль линии, но и необходимостью защитить расположенные рядом ВЧ цепи от взаимных мешающих влияний. Кабельные диэлектрики выбирают исходя из требования обеспечения наибольшей дальности связи в каналах ВЧ при минимальных потерях.

В соответствии с этим кабельная техника развивается в следующих направлениях:

- Преимущественное развитие коаксиальных систем, позволяющих организовать мощные пучки связи и передачу программ телевидения на большие расстояния по однокабельной системе связи.
- Создание и внедрение перспективных ОК связи, обеспечивающих получение большого числа каналов и не требующих для своего производства дефицитных металлов (медь, свинец).
- Широкое внедрение в кабельную технику пластмасс (полиэтилена, полистирола, полипропилена и др.), обладающих хорошими электрическими и механическими характеристиками и позволяющих автоматизировать производство.
- Внедрение алюминиевых, стальных и пластмассовых оболочек вместо свинцовых. Оболочки должны обладать

герметичностью и обеспечивать стабильность электрических параметров кабеля в течение всего срока службы.

- Разработка и внедрение в производство экономичных конструкций кабелей внутризоновой связи (однокоаксиальных, одночетверочных, безбронных).
- Создание экранированных кабелей, надежно защищающих передаваемую по ним информацию от внешних электромагнитных влияний и грозы, в частности кабелей в двухслойных оболочках типа алюминий — сталь и алюминий — свинец.
- Повышение электрической прочности изоляции кабелей связи. Современный кабель должен обладать одновременно свойствами как высокочастотного кабеля, так и силового электрического кабеля, и обеспечивать передачу токов высокого напряжения для дистанционного электропитания необслуживаемых усилительных пунктов на большие расстояния.

Конструкция и характеристика оптических кабелей связи

Классификация оптических кабелей связи

Оптический кабель состоит из скрученных по определенной системе оптических волокон из кварцевого стекла (световодов), заключенных в общую защитную оболочку. При необходимости кабель может содержать силовые (упрочняющие) и демпфирующие элементы.

Существующие ОК по своему назначению могут быть классифицированы на три группы: магистральные, зоновые и городские. В отдельные группы выделяется подводные, объектовые и монтажные ОК.

Магистральные ОК предназначаются для передачи информации на большие расстояния и значительное число каналов. Они должны обладать малыми затуханием и дисперсией и большой информационно-пропускной способностью. Используется одномодовое волокно с размерами сердцевины и оболочки 8/125 мкм. Длина волны 1,3...1,55 мкм.

Зоновые ОК служат для организации многоканальной связи между областным центром и районами с дальностью связи до 250 км. Используются градиентные волокна с размерами 50/125 мкм. Длина волны 1,3 мкм.

Городские ОК применяются в качестве соединительных между городскими АТС и узлами связи. Они рассчитаны на короткие расстояния (до 10 км) и большое число каналов. Волокна-градиентные (50/125 мкм). Длина волны 0,85 и 1,3 мкм. Эти линии, как правило, работают без промежуточных линейных регенераторов.

Подводные ОК предназначаются для осуществления связи через большие водные преграды. Они должны обладать высокой механической прочностью на разрыв и иметь надежные влагостойкие покрытия. Для подводной связи также важно иметь малое затухание и большие длины регенерационных участков.

Объектовые ОК служат для передачи информации внутри объекта. Сюда относятся учрежденческая и видеотелефонная связь, внутренняя сеть кабельного телевидения, а также бортовые информационные системы подвижных объектов (самолет, корабль и др.).

Монтажные ОК используются для внутри- и межблочного монтажа аппаратуры. Они выполняются в виде жгутов или плоских лент.

Оптические волокна и особенности их изготовления

Основным элементом ОК является оптическое волокно (световод), выполненное в виде тонкого стеклянного волокна цилиндрической формы, по которому передаются световые сигналы с длинами волны 0,85...1,6 мкм, что соответствует диапазону частот (2,3...1,2) • 10^{14} Гц.

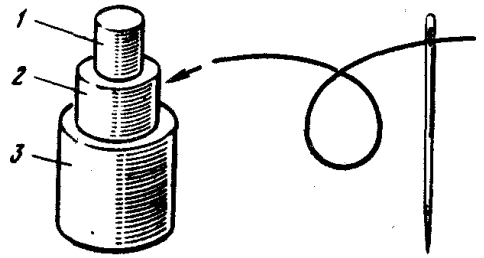
Световод имеет двухслойную конструкцию и состоит из сердцевины и оболочки с разными показателями преломления (n1 и n2). Сердцевина служит для передачи электромагнитной энергии. Назначение оболочки — создание лучших условий отражения на границе «сердцевина — оболочка» и защита от помех из окружающего пространства.

Сердцевина волокна, как правило, состоит из кварца, а оболочка может быть кварцевая или полимерная. Первое волокно называется кварц—кварц, а второе кварц—полимер (кремнеорганический компаунд). Исходя из физико-оптических характеристик предпочтение отдается первому. Кварцевое стекло обладает следующими свойствами: показатель преломления 1,46, коэффициент теплопроводности 1,4 Вт/мк, плотность 2203 кг/м^3.

Снаружи световода располагается защитное покрытие для предохранения его от механических воздействий и нанесения расцветки. Защитное покрытие обычно изготавливается двухслойным: вначале кремнеорганический компаунд (СИЭЛ), а затем — эпоксидакрылат,

фторопласт, нейлон, полиэтилен или лак. Общий диаметр волокна 500...800 мкм.

Сечение оптического волокна:



1— сердцевина; 2 — оболочка; 3 — защитное покрытие

В существующих конструкциях ОК применяются световоды трех типов: ступенчатые с диаметром сердцевины 50 мкм, градиентные со сложным (параболическим) профилем показателя преломления сердцевины и одномодовые с тонкой сердцевиной (6...8 мкм).

По частотно-пропускной способности и дальности передачи лучшими являются одномодовые световоды, а худшими — ступенчатые.

Важнейшая проблема оптической связи — создание оптических волокон (ОВ) с малыми потерями. В качестве исходного материала для изготовления ОВ используется кварцевое стекло, которое является хорошей средой для распространения световой энергии. Однако, как правило, стекло содержит большое количество посторонних примесей, таких как металлы (железо, кобальт, никель, медь) и гидроксильные группы (ОН). Эти примеси приводят к существенному увеличению потерь за счет поглощения и рассеяния света. Для получения ОВ с малыми потерями и затуханием необходимо избавиться от примесей, чтобы было химически чистое стекло.

В настоящее время наиболее распространен метод создания ОВ с малыми потерями путем химического осаждения из газовой фазы.

Получение ОВ путем химического осаждения из газовой фазы выполняется в два этапа: изготовляется двухслойная кварцевая заготовка и из нее вытягивается волокно.

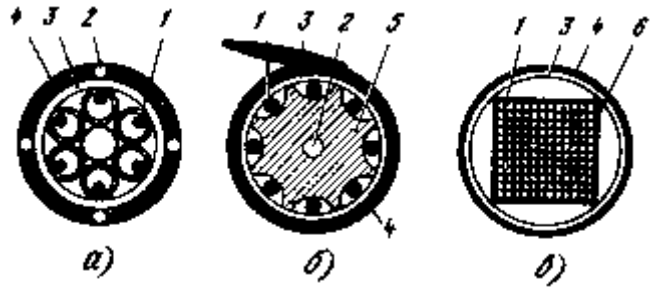
Во внутрь полой кварцевой трубки с показателем преломления n2 длиной 0,5...2 м и диаметром 16...18 мм подается струя хлорированного кварца и кислорода. В результате химической реакции при высокой тем-

пературе (1500...1700°С) на внутренней поверхности трубки слоями осаждается чистый кварц. Таким образом, заполняется вся внутренняя полость трубки, кроме самого центра. Чтобы ликвидировать этот воздушный канал, подается еще более высокая температура (1900°С), за счет которой происходит ухлопывание и трубчатая заготовка превращается в сплошную цилиндрическую заготовку. Чистый осажденный кварц затем становится сердечником ОВ с показателем преломления n1, а сама трубка выполняет роль оболочки с показателем преломления n2. Вытяжка волокна из заготовки и намотка его на приемный барабан производятся при температуре размягчения стекла (1800...2200°С). Из заготовки длиной в 1 м получается свыше 1 км оптического волокна.

Достоинством данного способа является не только получение ОВ с сердечником из химически чистого кварца, но и возможность создания градиентных волокон с заданным профилем показателя преломления. Это осуществляется: за счет применения легированного кварца с присадкой титана, германия, бора, фосфора или других реагентов. В зависимости от применяемой присадки показатель преломления волокна может изменяться. Так, германий увеличивает, а бор уменьшает показатель преломления. Подбирая рецептуру легированного кварца и соблюдая определенный объем присадки в осаждаемых на внутренней поверхности трубки слоях, можно обеспечить требуемый характер изменения по сечению сердечника волокна.

Конструкции оптических кабелей

Конструкции ОК в основном определяются назначением и областью их применения. В связи с этим имеется много конструктивных вариантов. В настоящее время в различных странах разрабатывается и изготавливается большое число типов кабелей.



Типовые конструкции оптических кабелей:

а — повивная концентрическая скрутка;

б — скрутка вокруг профилированного сердечника;

в — плоская конструкция;

1 — волокно;

2 — силовой элемент;

3 — демпфирующая оболочка;

4 — защитная оболочка;

5 — профилированный сердечник;

6 — ленты с волокнами.

Однако все многообразие существующих типов кабелей можно подразделять на три группы:

- кабели повивной концентрической скрутки;
- кабели с фигурным сердечником;
- плоские кабели ленточного типа.

Кабели первой группы имеют традиционную повивную концентрическую скрутку сердечника по аналогии с электрическими кабелями. Каждый последующий повив сердечника по сравнению с предыдущим имеет на шесть волокон больше. Известны такие кабели преимущественно с числом волокон 7, 12, 19. Чаще всего волокна располагаются в отдельных пластмассовых трубках, образуя модули.

Кабели второй группы имеют в центре фигурный пластмассовый сердечник с пазами, в которых размещаются ОВ. Пазы и соответственно волокна располагаются по геликоиде, и поэтому они не испытывают продольного воздействия на разрыв. Такие кабели могут содержать 4, 6, 8 и 10 волокон. Если необходимо иметь кабель большой емкости, то применяется несколько первичных модулей.

Кабель ленточного типа состоит из стопки плоских пластмассовых лент, в которые вмонтировано определенное число ОВ. Чаще всего в ленте располагается 12 волокон, а число лент составляет 6, 8 и 12. При 12 лентах такой кабель может содержать 144 волокна.

В оптических кабелях кроме ОВ, как правило, имеются следующие элементы:

- силовые (упрочняющие) стержни, воспринимающие на себя продольную нагрузку, на разрыв;
- заполнители в виде сплошных пластмассовых нитей;

- армирующие элементы, повышающие стойкость кабеля при механических воздействиях;
- наружные защитные оболочки, предохраняющие кабель от проникновения влаги, паров вредных веществ и внешних механических воздействий.

В России изготавливаются различные типы и конструкций ОК. Для организации многоканальной связи применяются в основном четырех- и восьмиволоконные кабели.

Представляют интерес ОК французского производства. Они, как правило, комплектуются из унифицированных модулей, состоящих из пластмассового стержня диаметром 4 мм с ребрами по периметру и десяти ОВ, расположенных по периферии этого стержня. Кабели содержат 1, 4, 7 таких модулей. Снаружи кабели имеют алюминиевую и затем полиэтиленовую оболочку.

Американский кабель, широко используемый на ГТС, представляет собой стопку плоских пластмассовых лент, содержащих по 12 ОВ. Кабель может иметь от 4 до 12 лент, содержащих 48–144 волокна.

В Англии построена опытная линия электропередачи с фазными проводами, содержащими ОВ для, технологической связи вдоль ЛЭП. В центре провода ЛЭП располагаются четыре ОВ.

Применяются также подвесные ОК. Они имеют металлический трос, встроенный в кабельную оболочку. Кабели предназначаются для подвески по опорам воздушных линий и стенам зданий.

Для подводной связи проектируются ОК, как правило, с наружным броневым покровом из стальных проволок. В центре располагается модуль с шестью ОВ. Кабель имеет медную или алюминиевую трубку. По цепи «трубка—вода» подается ток дистанционного питания на подводные необслуживаемые усилительные пункты.

Оптические кабели российского производства

Первое поколение ОК, созданных в 1986–1988 гг., включает кабели городской (ОК-50), зоновой (ОЗКГ) и магистральной (ОМЗКГ) связи. Современные требования развития связи потребовали создания новых усовершенствованных типов ОК (второе поколение). Такими кабелями, разработанными в период 1990–1992 гг., являются: ОКК — для городской связи (прокладка в канализации), ОКЗ — для зоновой и ОКЛ — для линейной магистральной связи.

Отличительные особенности ОК второго поколения:

- переход на волны 1,3 и 1,55 мкм;
- применение одномодовых волокон;
- модульные конструкции кабелей (каждый модуль на 1, 2, 4 волокна);
- наличие медных жил для дистанционного электропитания;
- разнообразие типов наружных оболочек (стальные ленты, проволоки, стеклопластик, полиэтилен, оплетка);
- широкополосность и большие длины регенерационных участков.

Кабель ОКК по сравнению с ОК-50 имеет меньшее затухание, большие дальность связи и широкополосность. Кабель ОКК состоит из градиентных и одномодовых волокон.

Новый зоновый кабель ОКЗ имеет различные типы оболочек, позволяющих использовать его в различных условиях эксплуатации (земля, вода, подвеска).

Кабель междугородной связи ОКЛ по сравнению с предшествующим (ОМЗКГ) обладает большей длиной трансляционного участка и позволяет применять наиболее мощную систему передачи на 7680 каналов («Сопка-5»).

Рассмотрим конструкции отечественных ОК.

Кабель городской связи типа ОК-50 содержит четыре или восемь волокон. Волокна свободно расположены в полимерных трубках. Скрутка — повивная, концентрическая. В центре размещен силовой элемент из высокопрочных полимерных нитей. Снаружи имеется, полиэтиленовая оболочка.

Четырехволоконный кабель ОК-4 имеет принципиально ту же конструкцию и размеры, что и восьмиволоконный, но только четыре волокна в нем заменены пластмассовыми стержнями. Изготавливаются также кабели, содержащие больше число волокон. Городские кабели прокладываются в телефонные канализации.

Кабель городской связи типа ОКК, прокладываемый в канализации, содержит 4, 8 или 16 волокон. Кабель имеет градиентные волокна с диаметром сердцевины 50 мкм (ОКК-50-01) или одномодовые волокна с диаметром сердцевины 10 мкм (ОКК-10-02).

Силовой центральный элемент выполнен из стеклопластиковых стержней или стального троса, изолированного полиэтиленом. Поверх наложена скрутка из восьми оптических модулей или корделей. В каждом модуле может содержаться 1, 2 или 4 ОВ. Затем наложены фторопластная лента и полиэтиленовый шланг.

Кабели, предназначенные для прокладки в грунтах, зараженных грызунами или подверженных механическим воздействиям, имеют еще броневой покров из стеклопластиковых стержней, а поверх него — полиэтиленовый шланг (ОККС). Известны конструкции, в которых вместо стержней применяется оплетка (ОККО).

Для подводных речных переходов применяется кабель в алюминиевой оболочке с броневым покровом из круглых стальных проволок и полиэтиленовым шлангом (ОККАК). Для станционных вводов и монтажа создан кабель ОКС.

Кабель зоновой связи марки ОЗКГ содержит восемь градиентных волокон, расположенных в пазах профилированного пластмассового сердечника. Так как кабель предназначен для непосредственной прокладки в грунт, он имеет защитный броневой покров из стальных проволок диаметром 1,2 мм. Дистанционное электропитание регенераторов осуществляется по четырем медным изолированным проводникам диаметром 1,2 мм, расположенным в броневом покрове кабеля. Снаружи кабель имеет полиэтиленовую оболочку.

Зоновый кабель ОКЗ содержит четыре или восемь многомодовых ОВ, расположенных в четырех модулях сердечника кабеля, покрытых снаружи полиэтиленовой оболочкой. Кабель предназначен для прокладки в грунт, поэтому имеет защитный броневой покров. Возможны различные варианты брони: стальные круглые проволоки (ОКЗК), бронеленты (ОКЗБ), стеклопластиковые стержни (ОКЗС), стальная оплетка (ОКЗО). Изготовляются также подводные кабели с алюминиевой оболочкой и круглой стальной броней (ОКЗАК). Станционные кабели маркируются ОКС.

Дистанционное электропитание регенераторов осуществляется по четырем медным изолированным проводникам диаметром 1,2 мм, расположенным в сердечнике кабеля.

Кабель магистральной связи ОМЗКГ содержит одномодовые волокна, обеспечивающие многоканальную связь на большие расстояния. Кабель содержит четыре или восемь волокон, расположенных в пазах профилированного пластмассового сердечника. Защитный покров изготавливается в двух модификациях: из стеклопластиковых стержней или стальных проволок. Снаружи имеется пластмассовая оболочка. Кабель предназначен для прокладки в грунт.

Магистральный кабель ОКЛ изготавливается из одномодовых волокон с сердцевиной диаметром 10 мкм, имеет две модификации: с медными проводниками диаметром 1,2 мм для дистанционного питания регенераторов и без медных проводников с питанием от местной сети или автономных источников теплоэлектрогенераторов (ТЭГ).

Центральный силовой элемент выполнен из стеклопластиковых стержней. Наружный покров кабеля имеет несколько разновидностей: для прокладки в канализации — это полиэтиленовый шланг (марка ОКЛ), для подземной прокладки — броневой покров из стеклопластиковых стержней (ОКЛС), стальных лент (марка ОКЛБ), круглой проволоки (ОКЛК).

Для подводных речных переходов создан кабель с алюминиевой оболочкой и круглопроволочной броней (ОКЛАК). Для станционных вводов и монтажа используется кабель ОКС.

Основные направления развития и применения волоконной оптики

Открылись широкие горизонты практического применения ОК и волоконно-оптических систем передачи в таких отраслях народного хозяйства, как радиоэлектроника, информатика, связь, вычислительная техника, космос, медицина, голография, машиностроение, атомная энергетика и др. Волоконная оптика развивается по шести направлениям:

- многоканальные системы передачи информации;
- кабельное телевидение;
- локальные вычислительные сети;
- датчики и системы сбора обработки и передачи информации;
- связь и телемеханика на высоковольтных линиях;
- оборудование и монтаж мобильных объектов.

Многоканальные ВОСП начинают широко использоваться на магистральных и зоновых сетях связи страны, а также для устройства соединительных линий между городскими АТС. Объясняется это большой информационной способностью ОК и их высокой помехозащищенностью. Особенно эффективны и экономичны подводные оптические магистрали.

Применение оптических систем в кабельном телевидении обеспечивает высокое качество изображения и существенно расширяет возможности информационного обслуживания индивидуальных абонентов. В этом случае реализуется заказная система приема и предоставляется возможность абонентам получать на экране своих телевизоров изображения газетных полос, журнальных страниц и справочных данных из библиотеки и учебных центров.

На основе ОК создаются локальные вычислительные сети различной топологии (кольцевые, звездные и др.). Такие сети позволяют объединять вычислительные центры в единую информационную систему с большой пропускной способностью, повышенным качеством и защищенностью от несанкционированного допуска.

Волоконно-оптические датчики способны работать в агрессивных средах, надежны, малогабаритны и не подвержены электромагнитным воздействиям. Они позволяют оценивать на расстоянии различные физические величины (температуру, давление, ток и др.). Датчики используются в нефтегазовой промышленности, системах охранной и пожарной сигнализации, автомобильной технике и др.

Весьма перспективно применение ОК на высоковольтных линиях электропередачи (ЛЭП) для организации технологической связи и телемеханики. Оптические волокна встраиваются в фазу или трос. Здесь реализуется высокая защищенность каналов от электромагнитных воздействий ЛЭП и грозы.

Легкость, малогабаритность, невоспламеняемость ОК сделали их весьма полезными для монтажа и оборудования летательных аппаратов, судов и других мобильных устройств.

В последнее время появилось новое направление в развитии волоконно-оптической техники — использование среднего инфракрасного диапазона волн 2...10 мкм. Ожидается, что потери в этом диапазоне не будут превышать 0,02 дБ/км. Это позволит осуществить связь на большие расстояния с участками регенерации до 1000 км. Исследование фтористых и халькогенидных стекол с добавками циркония, бария и других соединений, обладающих сверхпрозрачностью в инфракрасном диапазоне волн, дает возможность еще больше увеличить длину регенерационного участка.

Ожидаются новые интересные результаты в использовании нелинейных оптических явлений, в частности соли тонного режима распространения оптических импульсов, когда импульс может распространяться без изменения формы или периодически менять свою форму в процессе распространения по световоду. Использование этого явления в

волоконных световодах позволит существенно увеличить объем передаваемой информации и дальность связи без применения ретрансляторов.

Весьма перспективна реализация в ВОЛС метода частотного разделения каналов, который заключается в том, что в световод одновременно вводится излучение от нескольких источников, работающих на разных частотах, а на приемном конце с помощью оптических фильтров происходит разделение сигналов. Такой метод разделения каналов в ВОЛС получил название спектрального уплотнения или мультиплексирования.

При построении абонентских сетей ВОЛС кроме традиционной структуры телефонной сети радиально-узлового типа предусматривается организация кольцевых сетей, обеспечивающих экономию кабеля.

Можно полагать, что в ВОСП второго поколения усиление и преобразование сигналов в регенераторах будут происходить на оптических частотах с применением элементов и схем интегральной оптики. Это упростит схемы регенерационных усилителей, улучшит их экономичность и надежность, снизит стоимость.

В третьем поколении ВОСП предполагается использовать преобразование речевых сигналов в оптические непосредственно с помощью акустических преобразователей. Уже разработан оптический телефон и проводятся работы по созданию принципиально новых АТС, коммутирующих световые, а не электрические сигналы. Имеются примеры создания многопозиционных быстродействующих оптических переключателей, которые могут использоваться для оптической коммутации.

На базе ОК и цифровых систем передачи создается интегральная сеть многоцелевого назначения, включающая различные виды передачи информации (телефонирование, телевидение, передача данных ЭВМ и АСУ, видеотелефон, фототелеграф, передача полос газет, сообщений из банков и т. д.). В качестве унифицированного принят цифровой канал ИКМ со скоростью передачи 64 Мбит/с (или 32 Мбит/с).

Для широкого применения ОК и ВОСП необходимо решить целый ряд задач. К ним прежде всего относятся следующие:

- проработка системных вопросов и определение технико-экономических показателей применения ОК на сетях связи;
- массовое промышленное изготовление одномодовых волокон, световодов и кабелей, а также оптоэлектронных устройств для них;

- повышение влагостойкости и надежности ОК за счет применения металлических оболочек и гидрофобного заполнения;
- освоение инфракрасного диапазона волн 2...10 мкм и новых материалов (фторидных и халькогенидных) для изготовления световодов, позволяющих осуществлять связь на большие расстояния;
- создание локальных сетей для вычислительной техники и информатики;
- разработка испытательной и измерительной аппаратуры, рефлектометров, тестеров, необходимых для производства ОК, настройки и эксплуатации ВОЛС;
- механизация технологии прокладки и автоматизация монтажа ОК;
- совершенствование технологии промышленного производства волоконных световодов и ОК, снижение их стоимости;
- исследование и внедрение солитонового режима передачи, при котором происходит сжатие импульса и снижается дисперсия;
- разработка и внедрение системы и аппаратуры спектрального уплотнения ОК;
- создание интегральной абонентской сети многоцелевого назначения;
- создание передатчиков и приемников, непосредственно преобразующих звук в свет и свет в звук;
- повышение степени интеграции элементов и создание быстродействующих узлов каналообразующей аппаратуры ИКМ с применением элементов интегральной оптики;
- создание оптических регенераторов без преобразования оптических сигналов в электрические;
- совершенствование передающих и приемных оптоэлектронных устройств для систем связи, освоение когерентного приема;

- разработка эффективных методов и устройств электропитания промежуточных регенераторов для зоновых и магистральных сетей связи;
- оптимизация структуры различных участков сети с учетом особенностей применения систем на ОК;
- совершенствование аппаратуры и методов для частотного и временного разделения сигналов, передаваемых по световодам;
- разработка системы и устройств оптической коммутации.

ISDN

ISDN — цифровая сеть с интеграцией услуг (Integrated Services Digital Network) — современное поколение всемирной телефонной сети. Поскольку ISDN использует цифровую технологию она может переносить любой тип информации, включая передачу речи высокого качества, быструю и корректную передачу данных от пользователя к пользователю.

Общие сведения об ISDN

Название сети Integrated Services Digital Network (ISDN) (Цифровая сеть с интеграцией услуг) относится к набору цифровых услуг, которые становятся доступными для конечных пользователей. ISDN предполагает оцифровывание телефонной сети для того, чтобы голос, информация, текст, графические изображения, музыка, видеосигналы и другие материальные источники могли быть переданы конечному пользователю по имеющимся телефонным проводам и получены им из одного терминала конечного пользователя. Сторонники ISDN рисуют картину сети мирового масштаба, во многом похожую на сегодняшнюю телефонную сеть, за тем исключением, что в ней используется передача цифрового сигнала и появляются новые разнообразные услуги.

ISDN является попыткой стандартизировать абонентские услуги, интерфейсы пользователь/сеть и сетевые и межсетевые возможности. Стандартизация абонентских услуг является попыткой гарантировать уровень совместимости в международном масштабе. Стандартизация интерфейса пользователь/сеть стимулирует разработку и сбыт на рынке этих интерфейсов изготовителями, являющимися третьей участвующей стороной. Стандартизация сетевых и межсетевых возможностей помогает в достижении цели возможного объединения в мировом масштабе путем обеспечения легкости связи сетей ISDN друг с другом.

Применения ISDN включают быстродействующие системы обработки изображений, дополнительные телефонные линии в домах для обслуживания индустрии дистанционного доступа, высокоскоростную передачу файлов и проведение видеоконференций. Передача голоса несомненно станет популярной прикладной программой для ISDN.

Многие коммерческие сети связи начинают предлагать ISDN по ценам ниже тарифных. В Северной Америке коммерческие сети связи с коммутатором локальных сетей (Local-exchange carrier) (LEC) начинают обеспечивать услуги ISDN в качестве альтернативы соединениям T1, которые в настоящее время выполняют большую часть услуг «глобальной телефонной службы» (WATS) (wide-area telephone service).

Предпосылки появления ISDN

В конце 60-х годов в ведущих западных странах начался активный процесс внедрения цифровых систем передачи на всех уровнях сети, которые благодаря своим улучшенным технико-экономическим показателям стали вытеснять аналоговые системы передачи. Практически, одновременно бурными темпами развивалась вычислительная техника, росло производство больших ЭВМ и все больше и больше предприятий переводило свои технологические процессы на компьютерную основу. Поскольку обработка и передача информации, как в компьютерной технике, так и в системах передачи имели одну и ту же природу, а именно, байтовую структуру, возникла хорошо обоснованная тенденция взаимного проникновения технологий связи и вычислительной техники, что привело к созданию цифровых систем коммутации с централизованным управлением по записанной программе.

Таким образом, можно отметить, что «неторопливая» эволюция систем связи с момента изобретения Беллом телефона в течение многих десятилетий до начала семидесятых годов прервалась революционными изменениями. А подлинный технологический «взрыв» в прогрессе развития телекоммуникационных систем вызвало изобретение микропроцессоров в середине семидесятых годов. Ведущие западные фирмы-разработчики оборудования связи быстрыми темпами разработали и стали производить системы коммутации с распределенным управлением, которые, практически, по всем параметрам превосходили предыдущее поколение систем коммутации, и новые модернизированные системы цифровой передачи. Компьютеры становились все меньше и меньше по размерам, производительность их росла и стала сравнима с производительностью больших ЭВМ, а их стоимость падала. Немаловажным фактором развития микро-ЭВМ и появления персональных компьютеров, стала совместимость уже разработанного программного обеспечения с новой технологической базой.

К середине 80-х годов уже была практически создана инфраструктура цифровых каналов передачи и цифровых систем коммутации на местном, междугородном и международном уровнях сетей связи и совершенно естественно встал вопрос о цифровизации последнего участка аналоговой сети связи — абонентского доступа или как его стали называть операторы всего мира — «последней мили». Поскольку реконструкция абонентской сети, по общему мнению, является самой трудоемкой и дорогостоящей частью модернизации всей сети, а также самой массовой в части оборудования, то именно здесь развернулись самые широкие дискуссии о типе интерфейсов и перехлестнулись интересы самых различных фирм. Следует также отметить, что в цифровой среде передача речи и всех видов данных осуществляется единообразно, поэтому у многих разработчиков создалось мнение об интеграции передачи всех видов информации в одной сети связи.

Таким образом, были созданы предпосылки для создания ISDN и, наконец, в 1984 году появились первые рекомендации MKKTT, который попытался объединить многие мнения фирм-производителей оборудования связи в виде единых требований.

Первое соединение, интегрировавшее речь, передачу данных и видеоизображения, было осуществлено фирмой AT&T совместно с телефонной компанией Illinois Bell для своих заказчиков — корпорации McDonalds — через коммутируемую сеть общего пользования, оборудованную системами коммутации типа 5ESS, в декабре 1986 года. Без всякого сомнения, этот факт представляет собой историческое событие в развитии отрасли связи. Начиная с 1986 г. стали проводиться ежегодные международные научно-технические конференции по ISDN.

Однако спецификации MKKTT носили рекомендательный характер и допускали многозначность в некоторых положениях. Это привело к тому, что при их реализации различными фирмами-производителями произошли значительные расхождения в протоколах обмена и к нестыковке различных терминалов и систем коммутации. Свою негативную роль сыграла также протекционистская политика практически всех операторов. Создалось положение, когда из-за вышеперечисленных причин абонент ISDN Франции не мог связаться, например, с абонентом ISDN Англии, а международная сеть ISDN представляла собой отдельные «острова», не стыкующиеся друг с другом. Одновременно росла критика самой концепции ISDN со стороны представителей конкурирующих технологий (операторов сетей X.25, компаний, предоставляющих выделенные линии и т.д.). Количество абонентов ISDN росло очень медленно и многие уже решили, что были свидетелями «мертворожденного ребенка».

В 1988 году Комиссия Европейского экономического сообщества (ЕЭС) учредила Европейский институт стандартизации в области связи (ETSI), основной целью деятельности которого является разработка единых стандартов для всех стран ЕЭС. 22 страны ЕЭС подписали Меморандум о взаимопонимании, в соответствии с которым к концу 1993 года были выработаны стандарты, так называемой, Euro-ISDN. Что касается России, то позиция Министерства связи РФ заключается в аккредитации своего постоянного представителя в ETSI и выполнении разрабатываемых институтом стандартов с учетом национальных особенностей.

После появления стандартов ETSI процесс развития ISDN пошел бурными темпами и буквально за последние два года количество абонентов ISDN в некоторых странах (ФРГ, Франция, США) удвоилось. Так, например, на сети Deutsche Telecom в ФРГ, которая в настоящее время является практически полностью интегральной, количество абонентов ISDN приблизилось к 12% от общего числа абонентов телефонной сети и еще около 800000 стоят в очереди на подключение.

Таким образом, ISDN доказала свое право на существование и, представляя собой в первую очередь сеть, ориентированную на потребности делового мира, является одним из основных источников доходов для Операторов.

Услуги ISDN

Услуги Интерфейса базовой скорости (Basic Rate Interface) (BRI), обеспечиваемые ISDN, предлагают два B-канала и один D-канал (2B+D). Обслуживание B-каналом BRI осуществляется со скоростью 64 Kb/сек; оно предназначено для переноса управляющей информации и информации сигнализации, хотя при определенных обстоятельствах может поддерживать передачу информации пользователя. Протокол обмена сигналами D-канала включает Уровни 1–3 эталонной модели OSI. BRI обеспечивает также управление разметкой и другие непроизводительные операции, при этом общая скорость передачи битов доходит до 192 Kb/сек. Спецификацией физического уровня BRI является CCITT 1.430.

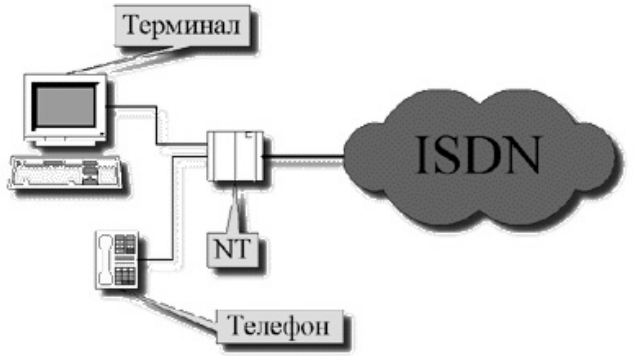
Услуги «Интерфейса первичной скорости» ISDN (Primary Rate Interface) (PRI) предлагают 23 B-канала и один D-канал в Северной Америке и Японии, обеспечивающие общую скорость передачи битов 1.544 Mb/сек (канал-D PRI работает на скорости 64 Kb/сек). PRI ISDN в Европе, Австралии и других частях света обеспечивает 30 B-каналов и один 64 Kb/сек D-канал и общую скорость интерфейса 2.048 Mb/сек. Спецификацией физического уровня PRI является CCITT 1.431.

Схемы подключения оборудования к ISDN-линии

Схема подключения оборудования зависит от условий работы, и от требований, которые пользователь предъявляет к линии.

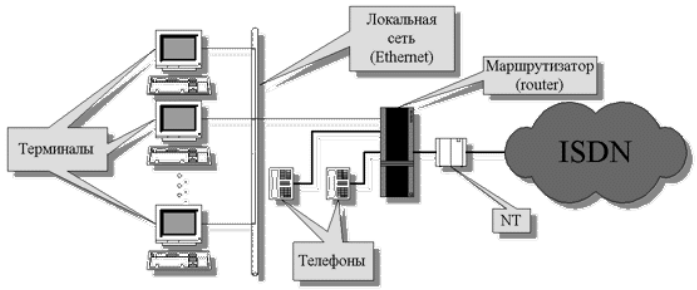
Существует три основных схемы подключения абонента:

1. Эту схему рекомендуется применять абонентам не имеющим локальной сети.



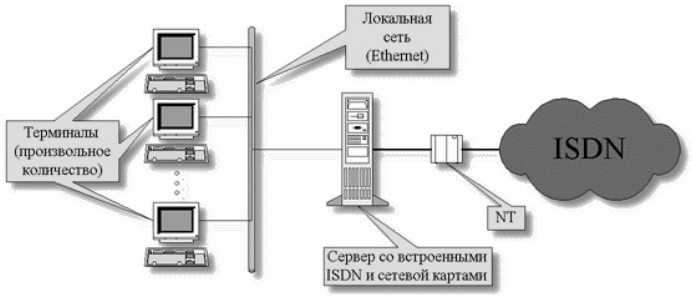
Как правило это люди которые проводят линию в квартиру, либо в офис, где в наличии имеется всего один терминал и один телефон. Эта схема реализуется при помощи ISDN-карты, которая играет роль маршрутизатора. Эта карта устанавливается в системный блок вашего компьютера, затем инсталлируется, и после этого ваш компьютер готов к работе с ISDN-линией. Затем необходимо соединить ваш терминал с сетевым окончанием (NT) посредством какого либо кабеля. Достоинство этого способа в дешевизне необходимого оборудования. В данном случае пользователю необходимо приобрести ISDN-карту с необходимым программным обеспечением для ее инсталляции (программное обеспечение должно прилагаться к карте при покупке), и кабель для подключения терминала к NT. Если вы хотите подключить телефон, вам необходимо так же приобрести переходник для подключения телефона к второму гнезду NT. Недостатком является то, что к линии можно подключить только один терминал.

2. Эту схему рекомендуется применять абонентам желающим подключить к линии небольшую локальную сеть.



Для осуществления этой схемы пользователю выделяется N+3-разрядная сеть, где N — количество ЭВМ в локальной сети. Это значит, что вам выдается N+3 свободных адреса, которые прописываются в сервере провайдера как ваши адреса. Но из этих N+3 адресов вы можете использовать только N, т.к. первый и последний не используются из-за технических особенностей сети (они используются как разделяющие), и еще один адрес присваивается маршрутизатору, который вам необходимо будет приобрести вместо использовавшейся в первом случае ISDN-карты. Достоинство маршрутизатора в том, что он в состоянии обслуживать сразу несколько терминалов. Так же в маршрутизаторе имеются два дополнительных гнезда для телефонов. Таким образом абонент получает возможность подключить N терминалов, 2 телефона, и при желании еще один телефон в NT (если имеется соответствующий переходник). Но для того чтобы объединить компьютеры в сеть, а затем эту сеть подключить к маршрутизатору, необходимо на каждый терминал установить сетевую карту, а затем объединить их в сеть кабелем. Т.е. для реализации данной схемы, необходимо приобрести маршрутизатор, сетевые карты, кабель и, по желанию, адаптеры для согласования телефонов с NT и с маршрутизатором. Сразу нужно отметить, что маршрутизатор примерно в 2 раза дороже ISDN-карты, самая дешевая сетевая карта стоит примерно 20$.

3. Эту схему рекомендуется применять большим предприятиям, количество терминалов которого значительно превышает 5.



Суть этого способа в том, что вместо маршрутизатора (как в предыдущем примере) используется отдельный сервер, устанавливаемый самим абонентом. Техническое исполнение не намного отличается от предыдущего примера. Во 2-м примере сеть, организованная абонентом, полностью прописывается в сервере и по сути дела является частью сети провайдера. В настоящем же примере в сервере представителя услуги прописывается лишь адрес сервера абонента, а сервер абонента прописывает все адреса абонентских терминалов. Теперь разрядность вашей локальной сети определяете вы сами, и разрядность эта может быть сколь угодно большой.

Для технической реализации этой схемы, необходимо приобрести прежде всего сервер. На этот компьютер ставится определенное программное обеспечение. Этот сервер будет исполнять роль маршрутизатора корпоративной сети. Сервер должен обслуживаться системным администратором. Затем необходимо приобрести и установить в сервер ISDN-карту (для подключения сервера к NT) и сетевую карту (для подключения к серверу — вашей сети). Так же необходимо приобрести сетевые карты для терминалов, входящих в состав вашей сети.

Сотовые системы связи. Терминология

Subscription fraud

Subscription fraud — преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты.

Subscription Fraud — подписное мошенничество (мошенничество с контрактом) — преднамеренное указание неверных данных при заключении контракта или невыполнение абонентом контрактных условий оплаты. Направлено на получение легального доступа к услугам сотовой связи с целью последующей не оплаты данных услуг. Примерами являются мошенничество с использованием заключенного контракта и мошенничество при использовании услуг льготного тарифа.

NITP — No Intention To Pay

NITP — No Intention To Pay — использование услуг связи без намерения платить за них.

Контракт (договор на оказание услуг связи) заключается без намерения оплачивать услуги. Данное деяние распространено в основном в регионах, где компании реализуют сотовые телефонные аппараты в кредит. Механизм таков, что злоумышленник приобретает телефонный аппарат в кредит чаще всего по подложным документам. Затем производит максимально возможное количество звонков (сам или предоставляет другим), а затем скрывается. Данное преступление возможно там, где не проверяются удостоверяющие личность данные. (Несмотря на то, что в России, в настоящее время, сотовые телефонные аппараты в кредит практически не продаются, операторы сотовой связи заключают договор на оказание услуг связи только на основании паспортных данных, что безусловно будет способствовать совершению подписного мошенничества). Так, например, в Великобритании, прежде чем продать телефон, работники компании сотовой связи проверяют соответствие личных, биографических данных, подлинность места жительства и семейно-имущественного статуса, профессионально-должностное положение потенциального клиента, а также его кредитоспособность на базе анализа банковских трансакций в течении последних пяти-шести лет. Информации о кредитном рейтинге оператор может получить у специализированных компаний, собирающих информацию за шесть последних лет практически по всему взрослому населению страны. Кредитный рейтинг клиента повышается, если он не имеет долгов, и понижается, если имеет трудности с возвратом долгов или прошел через процедуру банкротства.

Абоненты, заключившие контракт, принимают решение не оплачивать услуги в какой-то момент после начала действия контракта. В этом случае отмечается резкое изменение поведения абонента. Что касается первой категории, то для таких ситуаций нет надежных статистических данных, по которым их можно сравнивать и оценивать. Для оценки риска, связанного с такими абонентами, требуется дополнительная информация о них.

Мошенничество при использовании льготного тарифа включает два действия абонента-нарушителя: получение права пользования льготным тарифом некоторой службы и приобретение абонентом-нарушителем (или группой таких абонентов) нескольких номеров телефонов для того, чтобы звонить по номеру этой службы. В зависимости от схемы оплаты службы с льготным тарифом видоизменяются механизм мошенничества и его отличительные признаки. Если такая служба получает часть доходов от сети, то на ее номер поступают длительные повторяющиеся звонки. Если доход такой службы зависит от количества получаемых звонков, то ей поступает большое количество коротких звонков. Звонки на этот номер не будут оплачены.

Почти классический случай произошел недавно с одним из российских GSM-операторов. Злоумышленники зарегистрировали подставную компанию, арендовали платный номер во Франции и купили у российского оператора 50 телефонов, подключенных по кредитному тарифному плану. Затем они перевезли эти телефоны во Францию и поставили их на автодозвон до арендованного платного номера. Так они сгенерировали огромное количество очень дорогого трафика, приходящего на этот номер. В конце месяца France Telecom выплатил арендаторам номера несколько сотен тысяч долларов. Единственным пострадавшим от мошенников оказался российский сотовый оператор, которому французская компания выставила астрономические роуминговые счета — его ущерб составил около полумиллиона долларов.

Hacking fraud

Hacking fraud — проникновение хакеров в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы в своих целях

Hacking fraud — проникновение в компьютерную систему защиты для удаления механизмов защиты или переконфигурации системы базовых станций в целях использования (либо последующей продажи) имеющихся в системе функциональных возможностей.

Так как компьютерная информация системы сотовой связи (ESN и MIN номера) содержится в базовой станции и коммутаторе, то следующий способ неправомерного копирования может осуществляться через компьютерные сети. Данный способ во всех его вариациях очень широко описывался в научной литературе, поэтому мы не будем уделять ему внимание.

Другим видом данного способа являются действия сотрудников компании сотовой связи (нарушители) по внесению изменений в программное обеспечение компании, чтобы получить доступ к услугам по сниженной стоимости, либо без всякой оплаты.

На основании приведенной нами классификации следует подчеркнуть, что способы совершения сотового мошенничества имеют свои индивидуальные черты. Как правило, их основой являются действия преступника, направленные на получение различной степени доступа к системе сотовой связи (подготовительные действия по совершению мошенничества). В большинстве своем, все эти действия сопровождаются весьма квалифицированными способами маскировки, что само по себе затрудняет процесс выявления, раскрытия и расследования мошенничества. Исследование показало, что в большинстве случаев преступниками используются различные количественные и качественные комбинации нескольких способов. По мере их модификации и постоянного усложнения логических связей появляются новые способы, отличительной особенностью которых является уже наличие сложных алгоритмов действий преступника, которые все более совершенствуются и модернизируются.

Technical fraud

Technical fraud — неправомочное изготовление (клонирование) телефонных трубок или платежных телефонных карт с фальшивыми идентификаторами абонентов, номеров и платежных отметок

Technical Fraud — несанкционированное получение идентификационных данных пользователей с помощью технических средств с целью вмешательства, манипулирования или перепрограммирования идентификационных данных легальных пользователей. Мы полагаем, что данный способ совершения сотового мошенничества является разновидностью **Hacking fraud**, так как отечественная правоприменительная практика пошла по пути квалификации копирования идентификационных данных легальных пользователей систем сотовой связи с помощью технических средств по статье 272 УК РФ.

Наиболее общественно опасным и распространенным видом **Technical Fraud** является неправомерный доступ, повлекший копирование идентификационных данных пользователей системы сотовой связи.

Чаще всего, это происходит следующим образом: преступники перехватывают с помощью специального, сканирующего эфир оборудования, идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции и выделяют из него идентификационные номера. Наличие возможности перехвата идентификационных данных из эфира является недостатком всех аналоговых стандартов, например AMPS/D-AMPS без защиты A-Key и NMT-450 без SIS-кода.

Примером может служить следующее уголовное дело, которое было возбуждено 12 сентября 1997 г. УРОПД УВД Воронежской области. Предварительным следствием было установлено, что в мае 1997 г. гр. М.,

согласно разработанного плана, приобрел в г. Москве восемь сотовых аппаратов фирмы «МОТОРОЛА» и восемь микропроцессоров с специальной программой, позволяющих при монтаже в данные телефоны, получить аппараты с возможностями неправомерного доступа к компьютерной информации компаний сотовой связи, копирования личных и абонентских номеров законных пользователей компании, а также осуществления с данных аппаратов телефонных переговоров, оплата которых должна была осуществляться пользователями компании. Во исполнение своего преступного плана эти граждане с помощью переоборудованных аппаратов фирмы «МОТОРОЛА» в период с июля по ноябрь 1997 г. осуществляли неправомерный доступ к охраняемой законом компьютерной информации компании сотовой телефонной связи «ВОТЕК МОБАЙЛ» (стандарт — AMPS) и скопировали в г. Воронеже при помощи имеющихся у них переоборудованных аппаратов, 60 номеров законных пользователей данной компании. После этого, желая извлечь незаконную выгоду, неоднократно неправомерно получали доступ к компьютерной информации компании «ВОТЕК МОБАЙЛ», без оплаты осуществляли переговоры лично и предоставляли такую возможность третьим лицам.

Подобные примеры раскрытия и расследования Technical Fraud были в Москве, Нижнем Новгороде, Самаре и других городах. Одна из самых крупных в мире «краж» идентификационных данных при помощи сканирования зафиксирована в США. Два жителя Бруклина были арестованы за «кражу» (сканирование) 80 тысяч номеров сотовых телефонов у проезжих автомобилистов. Если бы эти номера удалось реализовать на «черном» рынке, ущерб от незаконно использованных телефонных услуг составил около 80 миллионов долларов.

Стандартными техническими средствами осуществления сканирования из эфира индивидуальных номеров пользователей являются следующие устройства и их комплексы (промышленного и кустарного производства):

а) Сотовый телефон с возможностью автосканирования. Для того, чтобы создать такой аппарат необходимо использовать два сотовых телефона, так как часть деталей одного аппарата задействуется как ЧИП автосканирования во втором. В аппарат впаивается ЧИП (после чего один из аппаратов становится неработоспособным), благодаря которому он после каждого разговора меняет частоту и номер, тем самым становясь практически недосягаемым для пеленгации и блокирования.

б) 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 сканирования практически невозможным. Разновидностью этого устройства являются мониторы сотовой связи, с помощью которых возможно не только сканирование индивидуальных номеров пользователей, но и прослушивание телефонных переговоров по сотовой связи.

Другой вид Technical Fraud заключается в получении идентификационных данных, либо их модификация (Access fraud) в результате непосредственного доступа к сотовому телефону. Для их изъятия возможен взлом алгоритмов, используемых для защиты персональной информации в телефонах.

Например, весной 2000 г. гражданин Д., имеющий специальные познания в области электроники и компьютерной техники, при помощи технических средств совершил доступ к охраняемой законом базе данных компьютерной информации пользователей, находящейся на машинном носителе в сети электронно-вычислительных машин компании мобильной связи. В своем офисе кустарным способом изготовил интерфейсы, предназначенные для связи компьютера через последовательный порт с телефоном LG-300, с целью неправомерного доступа к компьютерной информации. С помощью технических средств: интерфейса, компьютерной программы WLPST версии 1,7 осуществил копирование информации, содержащейся на микропроцессоре телефонного аппарата, а именно — личного номера пользователя, принадлежащего гражданину С. на свой телефонный аппарат LGC-300 ESN C603A913, то есть абонентского терминала, который является неотъемлемой частью компьютерной сети оператора сотовой связи, чем нарушил охраняемые законом права и интересы компании мобильной связи и произвел модификацию информации. По данному факту возбуждено уголовное дело по ч. 1 ст. 272 УК РФ.

Сравнительно новый тип фрода — это клонирование SIM-карт. После того как в апреле 1998 г. группе американских ученых удалось изготовить дубликат SIM-карты для телефона стандарта GSM, эта технология стала известна преступникам. «Для того чтобы клонировать чужую SIM-карту, требуется каким-то образом получить ее в свое распоряжение на шесть часов — столько времени нужно, чтобы подобрать код», — говорит Бернштейн. Телефоны устаревших стандартов NMT-450 и AMPS, в которых нет SIM-карт, клонировать еще проще — для этого достаточно сосканировать и выделить серийный номер телефона, передающийся по открытому радиоканалу, и присвоить его другому телефону. В стандарте GSM такое невозможно, и мошенникам необходимо физически получить SIM-карту.

Андрей Манешин, директор управления по борьбе с мошенничеством «ВымпелКома», заявил, что в сети «Би Лайн» не зафиксировано ни одного случая клонирования SIM-карт. От компании «Мобильные ТелеСистемы» не удалось получить комментариев на этот счет. По мнению начальника управления по борьбе с киберпреступностью ГУВД Москвы Дмитрия Чепчугова, не имея сообщников среди персонала сотовых операторов, создать дубли SIM-карт невозможно.

Как рассказал Чепчугов, недавно Управление «К» МВД задержало группу злоумышленников, торговавших дублями телефонов, принадлежащих крупным фирмам, имеющим большой объем трафика. Как правило, покупатели таких трубок организовывали в российских городах переговорные пункты, в течение 3–5 дней зарабатывали на этом деньги, а затем избавлялись от телефонов.

Procedural fraud

Procedural fraud — неправомочное использование роуминга и других бизнес-процедур (например, биллинга) с целью уменьшения оплаты услуг связи.

Доступ к системе сотовой связи с помощью использования знаний о процедурах ее функционирования

Procedural fraud — процедурное мошенничество. Все виды мошенничества этой категории включают атаки на процедурные алгоритмы, предназначенные для уменьшения риска мошенничества, и часто направлены на слабо защищенные места бизнес-процедур, используемых для предоставления доступа в систему. Примерами таких видов мошенничества являются неправомочное использование режимов роуминга, дублирование идентификаторов телефонных карт.

При мошенничестве в роуминге нарушитель учитывает, что процедура биллинга может производиться по истечении длительного времени после того, как были сделаны звонки, и в этом случае абонент-нарушитель может определенное время не получать счетов из-за задержек в биллинговых операциях. Существует еще одна ситуация при мошенничествах в роуминге, когда про абонента уже может стать известно, что он мошенничает, но ошибка в алгоритме аннулирования его контракта может дать ему возможность продолжать звонить, используя роуминг.

Что касается мошенничества с телефонными картами (Smart — карты — основаны на модуле идентификации пользователя SIM (Subscriber Identification Module) — модуль идентификации абонентов), то здесь мошенники используют слабые места в процедурах активизации и вывода из обращения оплаченных телефонных карт. Если информация о

предоплаченных картах становится достоянием ряда лиц, которые одновременно пытаются активизировать такие карты, то в случае, если имеется промежуток времени между кредитованием телефонного счета и выводом карты из обращения, фальшивые копии карт могут быть использованы несколькими лицами.

Stolen Phone Fraud

Stolen Phone Fraud — несанкционированное использование украденного сотового телефона законного пользователя. (Здесь мы предусматриваем также случаи, когда сотовый телефон изымается из владения легального пользователя иным уголовно наказуемым способом, например — грабеж, разбой и т.д.) Данное преступление ничем не отличается от обычной кражи. Однако цель его — использование телефона легального пользователя для подключения к системе сотовой связи и осуществление мошенничества в системе сотовой связи. Данный способ работает как правило, пока владелец не известит компанию и та не заблокирует доступ с украденного телефона. Например, по данным полиции Великобритании объектами краж и грабежей становятся 12,5 тысяч телефонов ежемесячно. 40% автомобильных взломов в центрах больших городов совершены ради телефонов, оставленных в салонах автомобилей их легальными владельцами. Причем, всего лишь за один день с помощью украденного телефона можно принести ущерб около 15 тысяч фунтов стерлингов

Staff fraud

Staff fraud — получение идентификационных данных пользователей с помощью сотрудников компаний сотовой связи для их последующего использования при программировании других телефонов (создания нелегального «двойника»). Так, в Москве раскрыто и расследовано уголовное дело, возбужденное по следующим обстоятельствам. Некий молодой человек регулярно размещал в Интернет объявления о том, что за 350 долларов готов изготовить сотовый телефон с возможностью только исходящей связи. В процессе расследования выяснилось, что у преступника был сообщник в одной из сотовых компаний, который предоставлял ему идентификационные данные легальных пользователей. В последствии, с помощью специальной программы преступник программировал в телефонные трубки полученные данные.

В Самаре, группа мошенников, владея секретной информацией, продавала сотовые телефоны, перепрограммированные на идентификационные данные легальных пользователей компании «Би Лайн-Самара». В процессе расследования выяснилось, что один из преступников работал инженером коммутатора компании «Би Лайн-Самара» и используя свое положение, получал идентификационные данные легальных пользователей.

Internal fraud

Internal fraud (внутреннее мошенничество) — неправомерное использование полномочий сотрудников компании-оператора для снижения стоимости услуг связи в личных целях. При осторожном использовании услуг данный способ мошенничества наиболее труден для обнаружения.

Система защиты PhonePrint (Corsair Communications Inc.)

PhonePrint (Corsair Communications Inc.) — комплекс распознавания радиотелефонов по радиоотпечаткам — Radio Frequency Fingerprint (уникальным характеристикам излучения передатчика каждого аппарата). Представители Fora Communications (AMPS), где PhonePrint был установлен в июле 97 года, утверждают, что система компании Corsair в целом работала успешно (стоимость составила около 1MUSD), однако уже в 98 году систему решили демонтировать и возвратить компании-производителю. Около 1/3 клиентов, отказавшихся от услуг Fora, испытывали неудобства от «двойников» с клонированными аппаратами. Fora вместо этого установила систему A-Key. По-видимому, следует ожидать вспышек «фрода» на региональных системах, куда «перетекут» клоны из С.-Петербурга. В 98.07 система PhonePrint введена в действие в Казахстане на системе Алтел. В 98.11 данная система была поставлена компанией Ericsson в Малайзию на сеть ETACS (55% сотового рынка).

В 99.01 Corsair подписал соглашение с Comcel (Colambia) на поставку системы PhonePrint 5.0, которая позволяет одной системой антифрода обслужить сразу несколько систем сотовой связи. В 99.02 состоялось подписание договора с ALLTEL — американским мультиоператором, обслуживающим более 6.5 млн. абонентов в 22 штатах. Если абонент данной сети переходит в режим роуминга, например, отправившись в другой город (при условии, что там также имеется система PhonePrint(R) 5.0), то местная система отправит «радиоотпечатки» излучения телефона в его «домашнюю систему». Связь состоится только в случае, если и роуминговая система и «домашняя система» будут располагать однотипной информацией. Если отпечатки совпадут, то звонок можно будет сделать. Несмотря на сложность сети, ожидание соединения для клиента не увеличивается, в то время, как любителей позвонить за чужой счет ждут трудные времена.

Система защиты A-Key

A-Key. Принцип работы: при включении радиотелефона компьютер сети передает на него случайное число. В телефоне число преобразуется по определенному алгоритму (CAVE — Cellular and Voice Encryption — американская технология шифрования аналогичная тем, что используется в военных целях) и направляется компьютеру (в HLR или AC — authentication Center). Компьютер выполняет те же действия с посланным числом, причем использует в качестве ключа то число, которое заранее в него занесено, как соответствующее данному телефонному аппарату. Результаты — вычисленный и присланный аппаратом сравниваются. Если результат совпадает, то телефон допускается в сеть. В каждом аппарате должен быть «зашит» индивидуальный A-Key. Поскольку A-ключ не передается в эфир, его нельзя перехватить и использовать, как это делалось с серийными номерами. В августе 98 данная система, закупленная у Motorola по цене 500.000 USD, запущена в компании Fora Communications (AMPS) (С.Петербург). Все новые телефоны уже снабжены A-Key, остальным клиентам необходимо было обратиться в офис компании за бесплатным перепрограммированием. Около 4000 телефонов ранних выпусков не поддерживают систему A-Key, их требуется заменить на новые, от клиентов потребуется доплата.

AKEY это тривиальное название системы аутентификации, используемой в сетях AMPS/DAMPS. Собственно AKEY представляет из себя восьмибайтовое число-ключ, хранящееся в сотовом телефоне абонента и являющееся уникальным для каждого абонента. AKEY вводится при продаже телефона клиента и хранится в базе. AKEY не меняется и остается постоянным при нормальной работе телефона. На основе AKEY (постоянный ключ) с помощью хеш-функции CAVE, использующей в качестве входных параметров, помимо AKEY, ESN, MIN телефона, а также случайное число, присланное по эфиру с базовой станции, генерируется временный ключ, называемый SSD_A (тоже 8 байт). Этот ключ в дальнейшем и используется при аутентификации для генерации ответного значения.

Постоянный AKEY не используется при аутентификации и служит только для расчета временного ключа. При установлении соединения система передает сотовому телефону случайное число, которое шифруется по алгоритму CAVE (Cellular Authentication and Voice Encryption) с использованием временного ключа SSD_A и других уникальных параметров телефона (ESN, MIN) в качестве ключа. Ответ посылается на базовую станцию, которая, в свою очередь, независимо от телефона генерирует ответное число (все параметры телефона, в том числе и AKEY, и текущий SSD_A, хранятся в базе на станции), и сравнивает его с полученным. В случае несовпадения числа, принятого от телефона

с независимо посчитанным числом, аутентификация считается неудачной и телефону отказывается в соединении.

Периодически (примерно раз в неделю) станция посылает сотовому телефону сообщения о генерации нового временного ключа, SSD_A, по получении этого сообщения (SSD_UPDATE) телефон рассчитывает новый временный ключ SSD_A, используя уже известный постоянный AKEY, ESN, MIN, и случайное число со станции. Таким образом, сам ключ аутентификации (SSD_A) является временным и периодически меняется, и становится бессмысленным «клонирование» трубок (а также нахождение SSD_A методом последовательного перебора), поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом.

Система защиты SIS — Subscriber Identification Security

Система SIS. SIS — Subscriber Identification Security. Внедрение началось на сетях NMT450 с системы «Дельта Телеком» еще в 1994 году. С тех пор, как утверждает менеджмент компании, не зарегистрировано ни одного случая проникновения в сеть. Внедрение функции было сложным и дорогостоящим и включало: модернизацию аппаратного и ПО коммутатора; приобретение и внедрение аппаратно-программного комплекса; замену всех мобильных аппаратов, не имевших встроенной функции SIS; модификацию ПО базовых станций. Соответствующая реализация стандарта известна под названием NMT450i. Помимо функции защиты от фрода, оператор получает ряд дополнительных возможностей, например, пониженный тариф для телефона с ограниченной (одной сотой) мобильностью, ограничение зоны обслуживания для конкретного абонента, SMS и ряд других. Основное преимущество — возможность организации автоматического роуминга.

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

Система защиты FraudBuster

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

Система защиты Signature Fraud Management System (Signature FMS)

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

Сетевые преступления. Терминология

QAH — Компьютерный абордаж

QAH — «Компьютерный абордаж» (хакинг — hacking): доступ в компьютер или сеть без нрава на то. Этот вид компьютерных преступлений обычно используется хакерами для проникновения в чужие информационные сети.

HACKER

1. Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум.

2. Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от теоретизирования по этому поводу.

Хакеры — это компьютерные хулиганы, одержимые «компьютерной болезнью» и ощущающие патологическое удовольствие от проникновения в чужие информационные сети.

QAI — перехват (interception)

QAI — перехват (interception): перехват при помощи технических средств, без права на то. Перехват информации осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключения к линиям периферийных устройств. При этом объектами непосредственного подслушивания являются кабельные и проводные системы, наземные микроволновые системы, системы спутниковой связи, а также специальные системы правительственной связи. К данному виду компьютерных преступлений также относится электромагнитный перехват (electromagnetic pickup). Современные технические средства позволяют получать информацию без непосредственною подключения к компьютерной системе: ее перехват осуществляется за счет излучения центрального процессора, дисплея, коммуникационных каналов, принтера и т.д. Все это можно осуществлять, находясь на достаточном удалении от объекта перехвата.

Для характеристики методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

- «Жучок» (bugging) — характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;
- «Откачивание данных» (data leakage) — отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;
- «Уборка мусора» (scavening) — характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности — физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.д. Электронный вариант требует исследования данных, оставленных в памяти машины;
- метод следования «За дураком» (piggbackiiig), характеризующий несанкционированное проникновение как в пространственные, так и в электронные закрытые

зоны. Его суть состоит в следующем. Если набрать в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

- метод «За хвост» (between the lines entry), используя который можно подключаться к линии связи законного пользователя и, догадавшись, когда последний заканчивает активный режим, осуществлять доступ к системе;
- метод «Неспешного выбора» (browsing). В этом случае несанкционированный доступ к базам данных и файлам законного пользователя осуществляется путем нахождения слабых мест в защите систем. Однажды обнаружив их, злоумышленник может спокойно читать и анализировать содержащуюся в системе информацию, копировать ее, возвращаться к ней по мере необходимости;
- метод «Поиск бреши» (trapdoor entry), при котором используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;
- метод «Люк» (trapdoor), являющийся развитием предыдущего. В найденной «бреши» программа «разрывается» и туда вставляется определенное число команд. По мере необходимости «люк» открывается, а встроенные команды автоматически осуществляют свою задачу;
- метод «Маскарад» (masquerading). В этом случае злоумышленник с использованием необходимых средств проникает в компьютерную систему, выдавая себя за законного пользователя;
- метод «Мистификация» (spoofing), который используется при случайном подключении «чужой» системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некоторую полезную для него информацию, например коды пользователя.

QAT — кража времени

QAT — кража времени: незаконное использование компьютерной системы или сети с намерением неуплаты.

QDL — QDT — логическая бомба (logic bomb)

QDL/QDT — логическая бомба (logic bomb), троянский конь (trojan horse): изменение компьютерных данных без права на то, путем внедрения логической бомбы или троянского коня. Логическая бомба заключается в тайном встраивании в программу набора команд, который должен сработать лишь однажды, но при определенных условиях.

Троянский конь — заключается в тайном введении в чужую программу таких команд, которые позволяют осуществлять иные, не планировавшиеся владельцем программы функции, но одновременно сохранять и прежнюю работоспособность.

QDV — вирус (virus)

QDV — вирус (virus): изменение компьютерных данных или программ, без права на то, путем внедрения или распространения компьютерного вируса.

Компьютерный вирус — это специально написанная программа, которая может «приписать» себя к другим программам (т.е. «заражать» их), размножаться и порождать новые вирусы для выполнения различных нежелательных действий на компьютере.

Процесс заражения компьютера программой-вирусом и его последующее лечение имеют ряд черт, свойственных медицинской практике. По крайней мере, эта терминология весьма близка к медицинской:

- резервирование — копирование FAT, ежедневное ведение архивов измененных файлов — это самый важный и основной метод защиты от вирусов. Остальные методы не могут заменить ежедневного архивирования, хотя и повышают общий уровень защиты;
- профилактика — раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение дисков на «непотопляемые отсеки» — зоны с установленным режимом «только для чтения», хранение неиспользуемых программ в архивах, использование специальной «инкубационной» зоны для записи новых программ с дискет, систематическая проверка BOOT-сектора используемых дискет и др.;

- анализ — ревизия вновь полученных программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами по меньшей мере на известные виды компьютерных вирусов и в течение определенного времени за ней должно быть организовано наблюдение;
- фильтрация — использование резидентных программ типа FluShot Plus, MaceVaccinee и других для обнаружения попыток выполнить несанкционированные действия;
- вакцинирование — специальная обработка файлов, дисков, каталогов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом вируса, для определения заряжения программы или всего диска;
- терапия — деактивация конкретного вируса в отраженных программах с помощью специальной антивирусной программы или восстановление первоначального состояния программ путем уничтожения всех экземпляров вируса в каждом из зараженных файлов или дисков с помощью программы-фага.

Понятно, что избавится от компьютерного вируса гораздо сложнее, чем обеспечить действенные меры по его профилактике.

Этот вид деяний является очень распространенным в настоящее время и может соперничать по количеству зарегистрированных фактов разве что только с неправомерным завладением информацией как товаром. Суть данного преступления заключается в написании специальной программы для ЭВМ, обладающей способностью многократного копирования себя и выполняющего другие заданные автором функции (осыпать буквы с экрана дисплея в одну кучу, проигрывать мелодию «Yankee Doodle» и т.п.).

Такой вид «интеллектуального хулиганства» получил широкое распространение в молодежной среде технических вузов, где способность написать программный вирус квалифицируется как барьер, после преодоления которого человек становится авторитетным специалистом в области системного программирования.

QDW — червь

QDW — червь: изменение компьютерных данных или программ, без права на то, путем передачи, внедрения или распространения компьютерного червя в компьютерную сеть.

QFC — компьютерные мошенничества

QFC — компьютерные мошенничества, связанные с хищением наличных денег из банкоматов.

QFF — компьютерные подделки

QFF — компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств (карточек и пр.).

QFG — мошенничества и хищения, связанные с игровыми автоматами

QFG — мошенничества и хищения, связанные с игровыми автоматами.

QFM — манипуляции с программами ввода-вывода

QFM — манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них путем манипуляции программами. В этот вид компьютерных преступлений включается метод Подмены данных кода (data diddling code change), который обычно осуществляется при вводе-выводе данных. Это простейший и потому очень часто применяемый способ.

QFP — компьютерные мошенничества и хищения

QFP — компьютерные мошенничества и хищения, связанные с платежными средствами. К этому виду относятся самые распространенные компьютерные преступления, связанные с кражей денежных средств, которые составляют около 45% всех преступлений, связанных с использованием ЭВМ.

QFT — телефонное мошенничество

QFT — телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

QRG/QRS — незаконное копирование

QRG/QRS — незаконное копирование, распространение или опубликование компьютерных игр и другого программного обеспечения, защищенного законом.

Неправомерное завладение информацией как товаром. Это наиболее распространенный вид преступных деяний, который заключается в копировании программ для ЭВМ или целой информационной системы (банка данных электронного архива и т.п.) без согласия (разрешения) владельца или собственника. Данный вид деяний очень широко распространен в нашей стране как практически единственная форма получения современного программного обеспечения.

Так, по данным экспертов, только одна из тысячи операционных систем Windows, функционировавших на персональных компьютерах с процессором Pentium, была приобретена на законных основаниях. Большинство органов государственной власти, в которых эксплуатируется данная операционная система, в том числе правоохранительные органы и органы, призванные обеспечивать информационную безопасность, никогда официально ее не приобретали. Такое положение определяется тем, что профессиональные пользователи не могут платить за новый программный продукт сумму, равную нескольким своим месячным заработным платам. В итоге это влечет появление спроса на деятельность по «взламыванию» систем противодействия несанкционированному копированию и его свободному распространению. Учитывая существующее экономическое положение России, можно предположить, что в ближайшие пять-десять лет ситуация коренным образом не изменится, несмотря на периодические попытки наведения порядка в данной сфере со стороны государства.

По словам одного из авторитетных программистов, в нашей стране существуют три основных способа распространения программных продуктов: воровство, грабеж и обмен краденным. Если не обращать внимания на юридические неточности в формулировке (которые можно простить программисту), то сложившаяся ситуация подмечена достаточно точно.

Примером такого преступления может быть переписывание программы расчета заработной платы, ведения главной книги бухгалтера, автоматизированного банка данных с адресами предприятий и т.п. При этом цель преступления — воспользоваться полезными свойствами неправомерно полученной информации (программы, базы данных): выполнить расчеты с использованием программы, получить справки, отчеты из баз данных и т.п.

С криминалистической точки зрения это уже более сложное деяние, для которого обязательно использование машинного носителя информации, так как современные программные продукты занимают весьма значительные объемы памяти. Для достижения целей данного вида действий часто бывает недостаточно завладеть только файлами программного продукта, так как для его нормального функционирования зачастую бывает необходимо наличие определенных компонент общего (драйверов периферийных устройств, наличия музыкальной карты и т.п.) или общесистемного программно-математического обеспечения (системы управления базами данных, электронной таблицы и т.п.).

Все три приведенные выше преступления имеют классификационный признак. Это означает, что их общей чертой является несанкционированное копирование компьютерной информации. Следовательно одной из основных задач расследования данных видов преступлений будет поиск и регистрация одинаковых (идентичных) наборов данных и программ в автоматизированной системе «жертвы» и «преступника».

QRT — незаконное копирование топографии

QRT — незаконное копирование топографии полупроводниковых изделий: копирование, без права на то, защищенной законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью, без права на то, топографии или самого полупроводникового изделия, произведенного с использованием данной топографии.

QSH — саботаж с использованием аппаратного обеспечения

QSH — саботаж с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

QSS — компьютерный саботаж с программным обеспечением

QSS — компьютерный саботаж с программным обеспечением: стирание, повреждение, ухудшение или подавление компьютерных данных или программ без права на то.

QZB — использование электронных досок объявлений

QZB — использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности.

QZE — хищение информации, составляющей коммерческую тайну

QZE — хищение информации, составляющей коммерческую тайну: приобретение незаконными средствами или передача информации, представляющей коммерческую тайну без права на то или другого законного обоснования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества.

QZS — использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера

QZS — использование компьютерных систем или сетей для хранения, обмена, распространения или перемещения информации конфиденциального характера.

Некоторые специалисты по компьютерной преступности в особую группу выделяют методы манипуляции, которые имеют специфические жаргонные названия.

Что взламывают, кто, и зачем…

Premium Rate Service, PRS

Premium Rate Service, PRS — Получение прибыли путем незаконного перевода вызовов на дорогостоящие каналы связи

Переадресация вызовов дальней связи на собственные каналы PRS, как правило — развернутые в других странах, позволяет мошенникам получать за счет оператора, из сети которого поступил вызов, внешне законную прибыль. Действительно, к поставщику дорогостоящей услуги деньги поступают от этого оператора независимо от того, оплатил абонент данную услугу или нет. Именно таким образом хакерская фирма, переводившая вызовы из Англии в собственные каналы в Израиле, в течение месяца «выкачала» из одного британского оператора 750 тыс. долл.

Простейшая схема переадресации услуг на линии PRS подразумевает участие сотрудников компании-жертвы. Например, в конце рабочего дня такой сотрудник дозванивается с определенных офисных телефонов до фирмы, предоставляющей услуги PRS, и оставляет аппарат в состоянии соединения на всю ночь. Работники, приходящие в офис утром, видят, что трубка одного телефонного аппарата (или нескольких) положена неаккуратно. Первое, что им приходит в голову: ее по неосторожности задел кто-то из технического персонала, производя уборку помещений по окончании рабочего дня.

Впрочем, встречаются и куда более изощренные варианты. Например, владелец одного из Web-серверов занимался тем, что незаметно для зашедшего на этот сервер пользователя модифицировал программное обеспечение, установленное на его компьютере, так что при повторном заходе на тот же сервер модемный доступ осуществлялся уже по дорогостоящему каналу (с тарифом 8 долл./мин!), причем новое соединение сохранялось в течение всего времени работы пользователя в Интернет. Ущерб от единичной акции такого рода равен примерно 5 тыс. долл., а максимальный «навар», который удалось получить мошенникам посредством переадресации сервиса, составил, согласно опубликованным данным, 60 млн. долл.

Call Selling

Call Selling — Продажа дорогостоящих чужих услуг по демпинговым ценам без оплаты счетов, приходящих от реального оператора

Действия, попадающие в категорию Call Selling, сегодня поставлены на индустриальную основу и контролируются крупными международными структурами. С целью «максимизировать» собственную прибыль мошенники интенсивно используют одну и ту же линию для множества международных переговоров — до тех пор, пока эта линия не будет отключена. В результате средний ежедневный ущерб оператора в пересчете на одну телефонную линию составляет 15 тыс. долл.

Создаваемый злоумышленниками трафик, который может проходить через несколько операторов, и, прежде всего через Ростелеком, является несанкционированным.

Корыстное хищение международного (междугородного) трафика актуально для всех направлений, но особенно — для международного трафика на Вьетнам, что объясняется двумя причинами:

- достаточно высоким тарифом для междугородных телефонных разговоров с Вьетнамом;

- наличием в России достаточно большой диаспоры выходцев из этого государства, ведущих здесь бизнес, что и обеспечивает постоянный спрос.

До настоящего момента не приходилось где-либо подробно ознакомиться с «вьетнамской» технологией для выработки практических мер по предотвращению возможного несанкционированного пропуска трафика. В том числе, нет подобных практических рекомендаций и в письмах, разосланных Ростелекомом в 2000–2001 гг. операторам связи «областного» масштаба. В них внимание акцентируется только на самом существовании проблемы.

Ниже будут рассмотрены три возможных алгоритма функционирования коммутаторных залов, которые реализуются или потенциально вполне реализуемы злоумышленниками (телефонными пиратами) на отечественных сетях электросвязи и соответствующие организационно-технические меры по пресечению несанкционированного трафика.

Одной из причин, обеспечивающей возможность функционирования «черных» коммутаторных залов является недоработка, допущенная в свое время разработчиками одночастотной системы сигнализации с частотой 2600 Гц.

Можно возразить, что одночастотная система сигнализации уходит в прошлое и что технология организации несанкционированного трафика, основанная на недостатках упомянутой сигнализации, теряет актуальность. Однако, одночастотная система будет использоваться еще довольно долго и фрикер, найдя слабое место, может причинить значительный ущерб оператору связи.

Сценарий 1. Возможный пропуск несанкционированного трафика посредством двух АМТС, расположенных в разных зонах

Устанавливается реальное, обычное междугородное соединение через две АМТС, которое фиксируется на АМТС «С», а также АТС «В» (если она оснащена системой повременного учета стоимости местных разговоров) и которое предназначено для тарификации. Как правило, это соединение по низкому тарифу.

Потом в результате процедуры «донабора» устанавливается нужное телефонному пирату международное соединение таким образом, что на АМТС «С» и на АТС «В» продолжается фиксация «обычного» междугородного соединения.

Реальная картина по трафику возможна только на АТС «D», но входящий междугородный трафик на АМТС, по существующей на отечественных сетях практике, детально не фиксируется и не тарифицируется, а на многих АМТС не фиксируется по техническим причинам.

Вывод. Необходимо программным путем закрыть транзит, пропуск трафика от «смежной АМТС» через АМТС на международную. То есть пропуск трафика по цепи C-D-M должен быть исключен для всех, в том числе операторов (телефонистов). Там, где по каким-либо причинам его исключить невозможно, он должен контролироваться.

Все изложенное применимо и к схеме, в которой АМТС «D» заменена на УАК.

Сценарий 2. Возможный пропуск несанкционированного трафика посредством двух АМТС, расположенных в одной зоне

В настоящее время часто приходится встречать размещение двух АМТС в одной зоне. Например, при модернизации сети, когда сеть как бы разделяется на две части — аналоговую и цифровую, оператор содержит две АМТС. Зона действия одной — цифровая часть сети, а другой — аналоговая часть. Внутризоновые соединения с одной части сети на другую происходят через перемычку между АМТС, которая часто строится с использованием междугородной одночастотной системы сигнализации.

Участок C-D в настоящем примере построен с использованием одночастотной системы сигнализации (D-C аналогично).

В этом случае так же производится «обычное» внутризоновое соединение (L-A-C-D-B-K) с использованием перемычки, далее производится «донабор» международного номера и установление международного соединения, причем тарификация на АМТС «С» будет как на внутризоновое соединение. В этом случае закрытие транзита будет не лучшим выходом из ситуации, так как транзит C-D-M (как и транзит D-C-M) открыт оператором преднамеренно для повышения использования ресурсов сети.

Автор рекомендует в этом случае постоянно контролировать трафик на перемычке, но не посредством тарификационных записей на АМТС. При первой фиксации появления несанкционированного трафика закрыть транзит C-D-M (как и транзит D-C-M). Со снижением коэффициента использования междугородных магистральных каналов (в том числе и на международную станцию) в этом случае придется смириться.

Сценарий 3.
Возможный пропуск несанкционированного трафика через АМТС, при заказных соединительных линиях (ЗСЛ), выполненных с использованием одночастотной системы сигнализации

Этот сценарий в техническом плане наиболее сложен для использования злоумышленниками. И меры по предотвращению несанкционированного трафика в настоящем случае трудоемки.

Так как в данном сценарии весь трафик (легальный и несанкционированный) идет через АМТС, то одной из мер борьбы автор предлагает подсчет и сверку всего трафика от зоны.

Для предотвращения пропуска несанкционированного трафика необходима целенаправленная работа в организационно-техническом плане:

- необходимо представлять места и маршруты несанкционированного пропуска трафика;
- необходимо производить контроль маршрутизации — транзитный пропуск трафика на АМТС, если он не обоснован, должен быть закрыт;
- на возможных путях и маршрутах пропуска несанкционированного трафика необходимо производить на регулярной основе мониторинг трафика (но не посредством тарификационных записей).

Клонирование терминалов сотовой связи

Когда были введены в действие первые аналоговые мобильные сети, то обеспечение безопасности в них было на очень низком уровне. По мере перехода от аналоговых к цифровым системам (GSM) менялся и характер мошенничества, поскольку нарушителям становилось все труднее (и, что более важно, дороже) перехватывать информацию и клонировать трубки. Это привело к переходу от технического мошенничества к процедурному и контрактному. 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 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.

Самым простым и доступным является контрактное мошенничество. В этой категории мошеннических действий услуги используются абонентами без какого-либо намерения платить за них. Мошенничества с использованием контракта весьма многообразны, но все ситуации можно разделить на две категории. Первая — когда контракт заключается без намерения оплачивать услуги, и вторая — когда абоненты, заключившие контракт, принимают решение не оплачивать услуги в какой-то момент после начала действия контракта. В этом случае отмечается резкое изменение поведения абонента. Что касается первой категории, то для таких ситуаций нет надежных статистических данных, по которым их можно сравнивать и оценивать. Для оценки риска, связанного с такими абонентами, требуется дополнительная информация о них. Такой вид мошенничества опасен только для оператора сотовой связи, абоненту он повредить не может.

Давайте разберемся с широко известным и очень «популярным» клонированием телефонов. Чтобы лучше понять проблемы, связанные с клонированием, давайте вспомним, что представляют собой сотовые телефоны и как работают.

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемопередающей радиостанцией. Каждому сотовому телефонному аппарату присваивается свой электронный серийный номер (ESN), который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот номер в руководстве для пользователя. При подключении аппарата к сотовой сети в микрочип телефона заносится еще и мобильный идентификационный номер (MIN). Вся территория, обслуживаемая сотовой системой связи, разделена на отдельные прилегающие друг к другу зоны связи или «соты». Телефонный обмен в каждой такой зоне управляется базовой станцией, способной принимать и передавать сигналы на большом количестве радиочастот. Периодически (с интервалом 30–60 минут) базовая станция излучает служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои MIN- и ESN-номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент времени.

Клонирование основано на том, что абонент использует чужой идентификационный номер (а, следовательно, и счет) в корыстных интересах. В связи с развитием быстродействующих цифровых сотовых технологий, способы мошенничества становятся все более изощренными,

но общая схема их такова: 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. Но не стоит пугаться и выбрасывать свой мобильник. Это только теория. На самом деле, все вышесказанное относится только к аналоговым стандартам (AMPS и NMT). В цифровых стандартах (GSM и DAMPS) базовая станция посылает случайный служебный сигнал, а телефон его шифрует и отправляет обратно. При этом, даже перехватив эту информацию, мошенники не смогут узнать код и перепрограммировать свой телефон. В апреле 1998 г. группа компьютерных экспертов из Калифорнии широко объявила и продемонстрировала, что ей удалось клонировать мобильный телефон стандарта GSM. Не так давно подобные технологии стали практиковать не только лаборатории, но и «подпольные» умельцы, на которых Россия особенно щедра.

Так можно или нет клонировать телефон GSM? Можно, но... Владельцам сотовых телефонов пока не следует особо беспокоится. Без физического доступа, по крайней мере, на несколько часов, их аппарат никто не сможет клонировать. Клонировать телефон, перехватывая информацию в эфире нельзя. Вот если вы потеряли свой телефон, а потом нашли (или вам его вернули) тогда будьте осторожны: не исключено, что у вашего мобильника появится двойник.

При использовании трубок-двойников возникают некоторые проблемы. Когда и мошенник (фрикер), и легальный абонент пытаются произвести звонок одновременно, тот, кто набрал номер первым, может разговаривать свободно, аппарат второго либо не найдет сеть, либо примет сигнал «номер занят». При попытке вместе ответить на входящий вызов оба аппарата сбросят звонок или вообще не будут подавать никаких сигналов. Нормально пользоваться связью можно только тогда, когда кто-то из двойников находится вне зоны покрытия или качество приема у одной из трубок на порядок выше, чем у другой. Поэтому обращайте внимание на подобные «мелочи». Но трубки-двойники не предоставляют полный контроль над телефонным номером и счетом. И тогда наиболее продвинутые фрикеры прибегают к опыту хакеров и «взламывают» системы учета клиентов, пользующихся услугами операторов сотовых сетей. Появляется «левый» абонент и его расчетный счет, к которому имеют доступ мошенники. Телефонный оператор не отличает его от остальных пользователей и полагает, что деньги на данном счету реально существуют. На самом же деле сумма — виртуальная. Это просто набор цифр. Биллинговые системы операторов ежедневно обрабатывают

огромное количество информации, и в общем, потоке проследить за легальностью всех операций практически невозможно. Потерянные таким образом суммы чаще всего списывают на ошибки сотрудников. Но это уже проблема для операторов, а не для абонентов, пусть сами разбираются, как им от этого защититься.

Какие выводы можно и нужно сделать любому абоненту? Прежде всего, владельцам сотовых телефонов GSM пока не следует особо беспокоится. Дублировать SIM-карты возможно, но для этого может потребоваться физический доступ к SIM-карте на время около 10 часов.

Для предотвращения мошенничества:

- узнайте у фирмы-производителя, какие средства против мошенничества интегрированы в ваш аппарат;
- держите документы с ESN-номером вашего телефона в надежном месте;
- ежемесячно и тщательно проверяйте счета на пользование сотовой связью (это основное);
- в случае кражи или пропажи вашего сотового телефона сразу предупредите фирму, предоставляющую вам услуги сотовой связи;
- держите телефон отключенным до того момента, пока вы не решили им воспользоваться. Этот способ самый легкий и дешевый, но следует помнить, что для опытного специалиста достаточно одного вашего выхода на связь, чтобы выявить MIN/ESN номера вашего аппарата (актуально для пользователей аналоговых систем сотовой связи);
- не пользуйтесь стандартами (фирмами): AMPS, AMT, Рус-Алтай, всеми видами транковой связи — все они легко взламываются хакерами. Пользуйтесь: D-AMPS (Билайн), GSM (GSM-900 и GSM-1800), и MNT-450i (хотя он и устаревший, но имеет ряд ценных качеств).

Tumbling

Технология Tumbling в среде клонирования абонентских терминалов сотовой связи

Чтобы обойти это препятствие, злоумышленники используют технологию «кувыркания» (tumbling) — вариант клонирования, при котором в телефон-копию закладываются идентификаторы сразу нескольких

(они могут исчисляться десятками) аппаратов-прототипов; при осуществлении вызова они выбираются поочередно. Указанная модификация уменьшает вероятность обнаружения клонированного телефона в сети и продлевает срок его службы до того момента, когда будет заблокирован последний из исходных идентификаторов. Телефоны, клонированные по методу tumbling, часто продаются на «сером» рынке с гарантией работоспособности в течение определенного срока; если трубка окажется заблокированной раньше, поставщик произведет бесплатную замену. Согласно имеющимся оценкам, в США ежемесячно клонируются около 75 тыс. телефонов, и, судя по всему, эта проблема исчезнет лишь тогда, когда аналоговые сотовые сети окончательно уйдут со сцены.

Мошенничество с телефонными картами

По оценкам компании PrKsidium Services, объем мирового рынка услуг сотовой связи с предоплатой уже превысил 2 млрд. долл. Возможность не заботиться о кредитной истории клиента и его текущей платежеспособности стимулирует повышенный интерес операторов к предоставлению услуг данного типа. Более того, оплата услуг с помощью телефонных карт избавляет операторов от процедур выставления счетов и контроля за их своевременной оплатой, а ведь не секрет, что биллинговые системы очень сложны в эксплуатации и довольно часто дают сбои.

Многие операторы считают продажу телефонных карт весьма эффективным способом привлечения новых клиентов, который, к тому же, снижает риск телефонного мошенничества.

К сожалению, последний тезис имеет мало общего с действительностью. Практически ничего не зная о абонентах, которые приобретают телефонные карты в самых разных местах, оператор открывает свою сеть для мошенников всех мастей. Не располагая многофункциональной биллинговой системой и надежными средствами администрирования, такой оператор зачастую даже не догадывается, каковы истинные масштабы ущерба, причиненного злоумышленниками. А его размеры составляют 3–5% суммарного дохода оператора, причем методы мошенничества учитывают специфику услуг с предоплатой.

Наиболее уязвимым местом является сама телефонная карта, а точнее, содержащийся на ней скрытый цифровой код. Нередки ситуации, когда этот код становится известен мошенникам еще до продажи карты, и ничего не подозревающий покупатель с удивлением обнаруживает, что бюджет только что приобретенной карты уже исчерпан. Украденные коды воспроизводятся на поддельных картах.

Что касается методов получения секретного кода, они на удивление просты. В одних случаях код просто может быть прочитан сквозь

целлофановую упаковку, в других эту упаковку можно вскрыть, а потом запечатать. Профессионалам удается даже стереть защитный слой на поле секретного кода, а затем восстановить его.

Невольными сообщниками мошенников нередко становятся сами изготовители телефонных карт. Секретные коды бывают неоправданно короткими, поэтому их без труда могут запоминать сотрудники, работающие на конвейере. Кроме того, им порой удается скопировать секретную информацию или попросту украсть ее для последующей продажи. Известен случай, когда якобы из-за сбоя печатающего устройства для большой партии карт были изготовлены двойники, содержавшие те же секретные коды. Карты-двойники поступили в розничную сеть наряду с оригиналами, и совокупный ущерб от этой «ошибки принтера» превысил 1 млн. долл.

Очень часто производитель рассматривает только что изготовленные карты как обычную печатную продукцию и не принимает специальных мер для обеспечения их безопасности при хранении и транспортировке. На деле же телефонные карты являются эквивалентом наличных денег (отличие заключается в том, что карты не могут служить средством платежа многократно).

Таким образом, введение телефонных карт в сетях мобильной связи просто перевело проблему мошенничества в иную плоскость. Услуги связи с предоплатой имеют ряд уникальных черт, поэтому здесь следует использовать специализированные системы обнаружения мошенничества. В любом случае оператор должен тщательно контролировать состояние балансов отдельных абонентов, пресекать любые попытки инициировать неразрешенные типы звонков, периодически генерировать и тщательно анализировать отчеты, содержащие параметры произведенных вызовов, внедрять надежные средства аутентификации абонентов. И конечно, он не имеет права игнорировать тенденцию, присущую сетям мобильной связи, в соответствии с которой простые методы мошенничества постепенно сменяются все более изощренными.

Шпионы — радиолюбители

Шпионы — радиолюбители незримы и очень опасны.

Любители коротковолновых радиопередач нередко натыкаются на загадочные станции, передающие бесконечные последовательности цифр. Непонятный код монотонно зачитывают на разных языках мужские, женские, а иногда и детские голоса. Странные передачи впервые появились в эфире около сорока лет назад; сигнал у подобных станций

весьма сильный, но они никогда не сообщают ни о месте своего расположения, ни об аудитории, для которой предназначена трансляция. Обычно слушатели, наткнувшись на такую передачу, какое-то время еще пытаются разобрать нескончаемое «три-пять-два-девять...», а потом, сбитые с толку, крутят ручку настройки дальше.

Крайне редко такие радиостанции передают отдельные фразы или тексты. Например, за несколько дней до роспуска восточногерманской внешней разведки «Штази» нестройный хор мужских голосов постоянно исполнял песенку про маленького утенка. Она транслировалась на тех же частотах, что и обычные указания «бойцам невидимого фронта».

Вокальные способности офицеров одной из самых эффективных разведок периода «холодной войны» смогли оценить по достоинству только многочисленные «нелегалы» и агенты из ГДР во всем мире: для них передача означала конец карьеры. Между тем песенку слышали не только разведчики и контрразведчики, но и многочисленные радиолюбители, которые, по всей вероятности, не понимали скрытого в ней смысла, зато педантично фиксировали время каждого сеанса и частоты «шпионских станций».

Одиночки против шпионов

Примерно с середины 1970-х годов, с появлением новых приемников с цифровыми устройствами для отслеживания передатчиков, коротковолновики-энтузиасты занялись «числовыми станциями» всерьез. К тому времени было уже ясно, что загадочные радиоточки принадлежат шпионским центрам и передают зашифрованные послания для своих агентов в других странах. Радиолюбители составили не только обширные перечни таких станций с точным расписанием их работы, но и занялись радиопеленгацией для установки мест их базирования.

Как известно, радиосвязь в диапазоне коротких волн обеспечивает трансляцию сообщений на максимально далекие расстояния, связывая между собой даже диаметрально противоположные точки земного шара. Соответственно КВ-радиопередачи представляют собой идеальный инструмент для анонимной односторонней связи. Агент разведки в любой точке планеты может получать послания от руководства с помощью маленького, общедоступного и никак не модифицированного радиоприемника.

Из многочисленных документальных книг и мемуаров отставных разведчиков уже давно известно, что для шифровки таких посланий используются так называемые одноразовые блокноты — криптосистема, абсолютно не вскрываемая при ее правильном использовании. Правда, истории известны и случаи роковых ошибок, когда «одноразовый» шифр

использовался многократно, что приводило к его вскрытию, чтению тайной переписки и аресту агентов.

Самая знаменитая история такого рода — американский «Проект Венона» (http://www.nsa.gov/docs/venona), приведший к разоблачению обширной сети советской разведки в 1940–50-х годах. Криптоаналитикам АНБ (Агентство национальной безопасности, NationalSecurityAgency, американский аналог российского ФАПСИ) удалось расшифровать часть сообщений, которыми обменивалась советская легальная резидентура с Центром.

Для тех, кто хочет превзойти АНБ, в Интернете существует оригинальный сайт Project Conet. Инициатором его стала небольшая британская компания Irdial-Discs, которая еще в 1997 году выпустила комплект из четырех компакт-дисков с записью передач шпионских «числовых станций» за последние тридцать лет. Теперь же, вдохновившись серией известных конкурсов RSA Challenges (соревнования по вскрытию секретных криптоключей популярных шифр-алгоритмов, проводимые компанией RSA), Project Conet (http://www.ibmpcug.co.uk/~irdial/conet.htm) призывает всех желающих заняться вскрытием шифрованных передач разведслужб. При этом в качестве объекта исследования избраны трансляции станций, расположенных в Британии, США и Германии.

Маловероятно, что разведки этих стран понесут какой-либо урон от действий интернетовских «криптоаналитиков». Вскрыть криптосистему такого уровня любителю не под силу. Скорее всего, столь своеобразной акцией компания просто пытается оживить интерес к несколько залежалому товару. Дело в том, что любой радиолюбитель может сам записать свежие передачи «числовых станций» или купить CD-ROM с такой подборкой. Интересно, впрочем, что, объявив конкурс, устроители почему-то забыли назвать сумму приза.

Радиоразведка (Communication Intelligence, COMINT) — самый старый вид радиоэлектронной разведки. Основное ее содержание — обнаружение и перехват открытых, засекреченных, кодированных передач связных радиостанций, пеленгование их сигналов, анализ и обработка добываемой информации с целью вскрытия ее содержания и определения местонахождения источников излучения. Сведения радиоразведки о неприятельских станциях, системах их построения и содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, устанавливать местонахождение их штабов и командных пунктов управления, баз и стартовых площадок ракетного оружия и так далее.

Вот три типичных примера сообщений подразделения радиотехнической разведки:

Российская военная сеть № 1

Трафик состоит из контрольных сеансов радиосвязи каждые два часа, хотя один раз случайно было передано зашифрованное сообщение.

Позывные: КАТОК-17, КАТОК-22, КАТОК-25, КАТОК-44, КАТОК-46, КАТОК-55, КАТОК-74, КАТОК-80, КАТОК-86, КАТОК-93, КАТОК-94, КАТОК-100, МАЛЕНЬКИЙ, БОЛЬШОЙ.

Частоты: 2650 кГц (Ночь), 5855 кГц (День).

Российская военная сеть № 2

Трафик в этой сети состоит из сообщений формата «5 цифр слово 4 цифры 4 цифры». Возможно, это разновидность зашифрованного сообщения.

Например: «54828 СВИНТУС 0064 0392» или «11233 БРОНЯ 2207 7720».

Позывные: КАЗАК-24, ВИРУС-11, УРОЖАЙ-24, ЭФИР-12.

Частоты: 4517 и 5794 кГц.

Российская военная сеть № 3

Трафик в этой сети состоит из обмена информацией между самолетами, кораблями и пунктом управления полетами (авиадиспетчером).

Позывные: КЛАД-86 (авиадиспетчер), МЕТЕОР-24 (самолет), НАГАН-58, КЛЕН-38, ВЕТЕР-41, ЛИДЕР-24, ГИПНОЗ-60, ЗИМА-158 (корабль).

Частоты: 5360 и 5888 кГц.

Эти данные взяты с одного из сайтов радиолюбителей — http://www.wunclub.com. Эти люди фанатично ищут любые секретные радиостанции, начиная с армий всех стран мира и заканчивая авиакосмическими агентствами. Понятно, что в списке есть и радиостанции агентов и нелегальных сотрудников разведок, будь то израильская, американская или российская. Множество радиолюбителей занимаются не только прослушиванием и записью передач «числовых станций», но и обычной радиоразведкой. Если в первом случае ущерб от их деятельности минимальный (технические подразделения контрразведки сами внимательно отслеживают все сеансы связи), то во втором они порой оказываются эффективнее военных. Ведь любители выполняют те же задачи, которые решает радиоразведка, но при этом у них есть уникальная возможность сравнивать данные, которые получены у не зависимых друг от друга операторов, чего не могут позволить себе военные.

Немного о призраках

Международный клуб радиолюбителей-перехватчиков «Spooks» («Привидения») предпочитает не афишировать себя. По своим техническим возможностям и эффективности работы «привидения» смело могут соперничать с радиоразведками ведущих мировых держав. Деятельность клуба началась в 1980-е годы, когда множество радиолюбителей по всему миру стали активно общаться между собой. В середине 1990-х часть из них увлеклась радиоразведкой. «Привидений» интересовали не только местоположение и параметры (расписание передач, позывные, частоты) отдельных радиостанций, в первую очередь военного назначения, но и содержание сообщений.

В отличие от СССР и впоследствии России, в США нет запрещенных для прослушивания частот (более того, там даже выпускают справочники с указанием частот наземных служб аэропортов, полиции, армии). В результате за долгие годы мониторинга эфира у членов клуба скопилась информация о том, как в какой период работал обнаруженный передатчик. То есть фактически каждый сам для себя занимался тем, что на языке радиотехнической разведки называется «составление графика активности». А это — полноценная часть работы разведки, которая позволяет при условии анализа многих данных прогнозировать события.

Вот что, например, Виктор Суворов писал в «Аквариуме» о возможностях радиоэлектронной разведки ГРУ: «На каждую радиостанцию, на каждый радар заводится дело: тип, назначение, где расположена, кому принадлежит, на каких частотах работает... Понятны нам сообщения или нет, на станцию заводится график активности и каждый ее выход в эфир фиксируется... Если каждый выход в эфир фиксировать и анализировать, то скоро становится возможным предсказывать ее поведение. В результате многолетнего анализа появляется возможность сказать: «Если вышла в эфир РБ-7665-1, значит, через четыре дня будет произведен массовый взлет в Рамштейне». Это нерушимый закон. А если вдруг заработает станция, которую мы называем Ц-1000, тут и ребенку ясно, что боеготовность американских войск в Европе будет повышена...».

Кто пользуется информацией, добытой «привидениями»? Кроме многочисленных сайтов радиолюбителей, которых сейчас насчитывается более тридцати, это журналисты, аналитики и все, кому нужна достоверная информация о ситуации в том или ином регионе. Хотя аналитическим возможностям «привидений» далеко до профессионалов из ГРУ, но кое-что могут и они. В качестве примера — история выявления группы российских агентов в США, бывших граждан Кубы.

Фантомы против кубинцев

28 сентября 1998 года на электронной доске объявлений клуба «Spooks» появилось сообщение: «Две недели тому назад газета Miami Herald сообщила, что агентами ФБР в Майами задержана группа кубинских шпионов, 12 человек, которые пытались проникнуть на американскую военную базу в Южной Флориде». Перед радиолюбителями была поставлена задача — установить, как сказался арест кубинских шпионов на активности радиопередатчиков, работающих с территории Кубы (именно задания такого рода в подобных ситуациях выполняют службы контрразведки).

Спустя неделю после ареста кубинских шпионов некто Энди Белл сообщил о том, что станция, которой любители дали номер S7 Russian Man, вдруг перешла на ежедневный режим работы. Как было установлено привидениями, до ареста шпионов передатчик выходил в эфир всего два раза в неделю. Исходя из этого, охотники предположили, что дублирование сообщений может означать, что получатель информации не отвечает на сигнал. Поскольку передатчик S7 Russian Man ранее проходил как принадлежащий ФАПСИ (под этим обозначением, помимо передатчиков собственно ФАПСИ, числятся радиостанции других российских разведывательных служб — СВР и ГРУ), то был сделан вывод, что кубинская группа, возможно, работала на русских. Далее (специально для интересующихся) была обнародована техническая информация, а именно частоты, на которых работал передатчик S7 Russian Man: 5937 кГц, 7737 кГц и 9337 кГц. По мнению некоторых экспертов, большинство передач для агентов российской разведки велось с Кубы, где до последнего времени находился центр радиоперехвата Лурдес. Выбор места не случаен: небольшое расстояние до территории США позволяло использовать маломощные компактные радиостанции для приема и передачи сообщений.

Радиолюбители всех стран

«Привидения» — не единственная организация подобного рода. В январе 1995 года начал действовать клуб WUN (WorldwideUTENews), о котором мы уже писали выше. Буквосочетание «UTE» означает, что членов клуба интересуют радиостанции, работающие в частотном диапазоне до 30 Мгц. Штаб WUN составляют 11 человек из США, Европы, Японии, Новой Зеландии, а простых участников насчитывается уже много больше сотни. На сегодняшний день почти не осталось мест на планете, которые не попали бы в их поле зрения.

Подобные организации — структура, о которой может только мечтать любая контрразведка или радиоразведка. Во-первых, они неуловимы: в качестве средства общения используют только электронную почту, работают обычно под псевдонимом, никогда сами не выходят в эфир, применяя только аппаратуру для радиомониторинга, благо во многих странах не требуется ее регистрация. В тех случаях, если регистрация официально нужна, как в России, необходимое оборудование всегда можно приобрести на «черном рынке».

Во-вторых, «привидения» и им подобные работают против других стран и тем самым не вступают в конфликт с местными правоохранительными органами. Например, американцы предпочитают слушать передатчики, находящиеся на Кубе, граждане Китая выбирают радиостанции США, а россияне — китайцев. Это связано не только с чувством патриотизма или инстинктом самосохранения, но и с техническими особенностями организации тайной радиосвязи.

В-третьих, для «призраков» характерен высокий уровень оперативности и достоверности. Благодаря «всемирной паутине» любая свежая информация почти мгновенно становится известна всем членам клуба. В-четвертых, радиолюбители исключительно профессиональны и внимательно изучают всю доступную информацию по организации радиоразведки и радиоэлектронной борьбы (РЭБ).

Несмотря на то, что многие отечественные радиолюбители активно участвуют в движение «призраков», о своих успехах они предпочитают распространяться только на англоязычных сайтах. Причина проста — нежелание вступать в конфликт с действующим российским законодательством. Например, в России существует довольно жесткая «Инструкция о порядке регистрации и эксплуатации любительских радиостанций». В ней не только регламентирована процедура регистрации радиостанций в органах Госсвязьнадзора, но и параметры (мощность, частота и т. п.) их устройства. Да и сама регистрация — процедура сложная, поэтому мало кто решается на нее. Зачем «призраку» регистрировать свой приемник, о существовании которого никто не узнает, если только сам хозяин не станет слишком хвастаться?

Другая особенность России — уголовная ответственность за использование специальных технических средств, предназначенных для негласного получения информации. Поясним, что речь идет о средствах радиомониторинга сетей пейджинговой, радио- и сотовой связи, например, о сканирующих приемниках и аналогичной аппаратуре. Понятно, что «призраков» не интересуют системы сотовой связи. А вот доказать это сотрудникам правоохранительных органов сложно. Это еще одна причина, из-за которой отечественные шпионы-радиолюбители предпочитают оставаться в тени.

И последний аспект феномена. Почему эти люди не работают на спецслужбы? Ответ прост. Они никому не нужны поодиночке. Это любители, которых трудно приучить к воинской дисциплине. Значит, их нужно призвать на военную службу. Каждый радиолюбитель может слушать лишь одну частоту и не больше шести часов в сутки, после чего внимание ослабевает. Следовательно, призраков должно быть много и каждый должен выполнять определенный объем работы. Чем же они тогда будут отличаться от обычных военнослужащих подразделений радиоэлектронной разведки?

Может быть, спецслужбам следует попытаться взять под контроль это движение? Проблема в том, что «призраки» обитают во многих странах, и у них нет формальных лидеров. Радиолюбителей можно назвать «хакерами эфира»: это своеобразный стиль жизни, мир, где каждый сам выбирает правила. Теоретически можно часть «призраков» завербовать, но станет ли от этого движение более управляемым?

На вопрос, пользуются ли спецслужбы результатами деятельности «призраков», нет однозначного ответа. Те государства, где нет мощных подразделений радиоразведки, несомненно, внимательно изучают все бюллетени. С развитыми странами сложнее. Несомненно, информацию «призраков» используют аналитики из спецслужб. А вот военные, скорее всего, предпочитают больше доверять собственным подразделениям радиоэлектронной разведки. Для армии важна не только достоверность, оперативность, но и полнота, чего «призраки» гарантировать никак не могут.

Варианты мошенничества

Вариант мошенничества путем съема квартиры

Способ до банальности прост и был распространен в основном в начале девяностых. Суть его очень проста:

Некие люди, милая семейка, желает снять квартирку «на длительное время». Для чего ищется квартира, подешевле и можно даже без мебели. Хозяева, обычно ни о чем не подозревающие люди, после переговоров заключают договор аренды, а иногда и просто достаточно устной договоренности, и взяв деньги за первый месяц спокойно отправляются восвояси, продумывая способы траты нажитых денег. Сразу замечу, что при данном варианте мошенничества, мошенник старается уговорить хозяев на помесячную оплату, т.е. без предоплаты за несколько месяцев. Опуская дальнейшие подробности, далее мошенник делает следующее:

В квартиру никто не въезжает, а просто привозится радио телефон дальнего радиуса действия и включается в телефонную розетку. После чего не трудно догадаться зачем это все проделано. В обычных случаях, неподалеку, оказывается либо гостиница либо несколько общежитий. В которых, собственно, мошенник и планирует «продать телефонную линию». Т.е. мошенник начинает продавать возможность позвонить по междугородней или международной связи несколько дешевле, чем на специальных переговорных пунктах. Этот способ получил громаднейшее распространение во время Олимпиады в Москве 1980-го года. По сути своей, этот способ настолько прост для мошенника, насколько прост для его предотвращения. Естественно, на сегодняшний день, таким образом, прокатить мало кого удастся.

Вариант мошенничества путем непосредственного подключения №1

Данный вариант мошенничества несколько сложнее, чем кажется на первый взгляд. Мошенник подключается к линии непосредственно в щитке, а еще хуже, вне Вашей лестничной клетки т.е. в подвале, в распределительной коробке Вашего дома, или совсем серьезней, в распределительном канале целого микрорайона (что крайне сильно усложняет вариант отлова мошенника). После установки соответствующего оборудования, мошенник начинает действовать, т.е. либо:

- продавать «межгород»;
- продавать «международку»;
- пытаться получить пиратский доступ «от вашего имени» к другим ресурсам телекоммуникационных сетей, естественно с целью достижения преступных замыслов.

Перехват трафика

Тип пиратства сводится к ситуации, когда тарификация за действительно предоставленную услугу связи реально происходит, но объектом для выставления счета становится посторонний абонент (заурядное несанкционированное подключение к абонентской линии, клонирование сотовых телефонов, «перехват эфира» у бытовых радиотелефонов, подмена АОН и т. д.). Для оператора связи это чревато не только убытками, но и негативными взаимоотношениями с абонентами. На основании рекламаций этих абонентов оператор связи в состоянии установить факт наличия фрикинга и оценить ущерб.

В результате деятельности телефонных пиратов второго типа тарификация за реальные услуги связи происходит неправильно, напри-

мер, международный телефонный разговор с государством Коста-Рика тарифицируется как междугородный разговор с городом Костромой. Разница тарифов и составляет доход телефонных пиратов. А в ряде случаев тарификации не происходит совсем. Этот тип пиратства опасен тем, что оператор связи, у которого происходит по сути хищение международного (междугородного) трафика, неопределенное время может и не догадываться об этом.

То есть трафик, создаваемый злоумышленниками, системами тарификации оператора контролируется не полностью, что создает почву не только для извлечения незаконной прибыли, но и для использования, например, террористами. Так же, в частности, посредством подобной технологии возможно дистанционное прослушивание местных телефонных разговоров.

Часть 2. Боксинг

BLUE BOX

Blue Box была так названа из-за цвета первого такого устройства. Устройство BB достаточно сложно и ее размер варьируется от размера современной ПЭВМ до пачки сигарет. BB содержит 12 или 13 кнопок, при нажатии на которые в телефонную линию испускается та или иная мульти-частота, соответствующая выбранной цифре.

BB делает возможным производить телефонные звонки без последующей оплаты услуг связи.

BB может быть непосредственно связана с телефонной линией, или может быть акустически соединена с ней посредством помещения динамической головки BB (если таковая имеется, и данный BB для этого предназначен) к микрофону телефонной трубки. Действие BB более подробно будет описано ниже.

Для понимания природы звонка BB необходимо понимать основное устройство и действие телефонной сети. Когда происходит запрос номера DDD должным образом, вызывающий номер будет определяться как неотъемлемая часть установления связи.

Это может быть выполнено автоматически (АОН) или, в некоторых случаях, при связи через телефонистку, вручную оператором (телефонисткой), которая спросит вызывающего абонента номер его телефона.

Эта информация поступает на устройство произвольного/последовательного доступа (УППД) АТС. На УППД будет содержаться вызываемый номер, вызывающий номер, время начала и конца звонка. Таким образом, в конце концов, тарификационная система АТС будет знать, что Вами был произведен звонок определенной длительности и по произведению месячного обсчета всех вызовов, Вам будет отправлен счет для оплаты за услуги связи.

Типичный пользователь BB обычно набирает номер, за который впоследствии платить не придется. Пользователь BB после получения доступа к телефонной сети использует кнопку BB для посылки тона час-

тотой 2600 Гц. Этот тон используется оборудованием переключения для освобождения линии вызывающего абонента (отбой).

Тон 2600 Гц является сигналом того, что вызывающий абонент повесил трубку. ВВ моделирует это условие. Однако фактически местный канал вызываемого абонента все еще остается на связи. Пользователь ВВ использует клавишу (ключ пульса) для уведомления переключающего оборудования АТС, что он собирается произвести набор номера. Пользователь набирает необходимый номер на ВВ. После этого он использует клавишу (старт), уведомляющую оборудование АТС, что передача сигналов завершена.

Если запрос завершен, то на УППД будет зарегистрирована только первая часть первоначального запроса до подачи сигнала 2600 Гц. Сигналы, испускаемые ВВ зарегистрированы не будут. Так как первоначальный запрос номера зарегистрирован не был, то за этим не следует никакого составления счетов за услуги связи.

Хотя все вышеупомянутое — описание типичного действия ВВ, использующим общий метод получения бесплатного доступа к телефонной сети, действие ВВ может быть другим в любом из следующих случаев:

1. ВВ может включать дисковый номеронабиратель для подачи сигналов 2600 Гц и сигналов переключения. Этот тип ВВ назван «Импульсным».

2. Связь с номером DDD может быть осуществлена путем перезапроса любой свободной транзитной линии общенациональной телефонной сети или международной сети, работающей или неработающей.

3. Связь с номером DDD может быть осуществлена также в форме «короткого» запроса. «Коротким» запросом называется тот, который приводит к меньшей сумме оплаты услуг связи, чем с помощью типового способа использования ВВ.

4. ВВ может быть установлен в разрыв телефонной линии или быть с ней акустически связанным. ВВ может быть даже встроена в телефон, использующий тональный набор.

5. Регистрация на УППД может производиться для записи сигналов ВВ определенного абонента, телефон которого используется вместо ВВ.

Все ВВ, кроме «Импульсных», должны иметь следующие 4 возможности:

1. Возможность подачи тонального сигнала частотой 2600 Гц.

2. ВВ должен иметь тон (ключ пульса), который готовит мультичастотный приемник для приема номера вызываемого телефона.

3. Типичный ВВ должен быть способен издавать тональные сигналы, используемые для передачи номера телефона. Каждая цифра телефонного номера представляется комбинацией 2-х тонов. Например, цифра 2 — комбинацией 700 Гц и 1100 Гц.

4. ВВ должен иметь клавишу, представленную комбинацией 2-х тонов, сообщающих оборудованию АТС, что передача телефонного номера завершена и оборудование должно начать вызывать запрошенный номер.

«Импульсному» ВВ необходим только дисковый номеронабиратель, посредством которого возможно подавать сигнал частотой 2600 Гц.

Blue Box использует тон в 2600 hz для управления телефонными переключателями, использующими полосу передачи сигналов. Абонент может затем обратиться к специальной функции переключателя, обычно с целью установления дальней телефонной связи, используя тона, обеспечиваемые Blue Box.

Иногда встречаются сообщения или ссылки на такую информацию: «Совместное использование ESS и Blue box невозможно». Это неверно. Когда я жил в штате Коннектикут, то запросто использовал Blue box под Step by Step, #1AESS и DMS-100. Это было действительно просто: даже если я инициализировал свое обращение к 800 номеру из разных мест (из офиса 5-го уровня, из здания финансовой биржи), то все равно звонок проходил через определитель суммы оплаты междугороднего разговора (New Haven № 5 Crossbar toll в главном офисе Tandem'a). На главной линии между 5-м уровнем (компания, офис) и 4-м уровнем (телефонная финчасть, в нашем случае New Haven #5 Xbar) для передачи сигналов использовалась полоса частот MF, и поэтому независимо от того, в какой город или регион я звонил, мое обращение шло по таким линиям, что я мог использовать свой Blue box хоть до посинения. Начальная АТС (SXS/ESS/ и т. д.) абсолютно не мешала мне включать Blue box.

Хотя появление ESS (и других электронных коммутаторов) сделало применение Blue box'ов несколько проблематичным, все же это не является причиной для отказа от использования этих устройств. Главная проблема скрыта в параметрах опции «forward audio mute» — одной из возможностей CCIS (вне несущей полосы). К сожалению, 99% служб, подобных упомянутой выше New Haven #5 Xbar, использует именно CCIS. Для большинства любителей Blue box'ов это настоящее бедствие. Пытаясь решить проблему, вы в поисках линии, использующей передачу сигналов в MF-частотах, неизбежно выйдете на блок сети, оборудован-

ный CCIS. Здесь вам надо найти коммутатор на 2600 hz. Главная ваша цель — так или иначе заполучить в свое распоряжение линии, где все еще используются MF-частоты для передача сигналов, но для этого вам придется как-то обходить или отключать опцию «audio mute» в CCIS. (Маленькая подсказка: приглядитесь поближе к WATS расширителям.)

BLACK BOX

Название Black Box (далее BlB) также происходит от цвета поверхности первого такого аппарата. Размер BlB непостоянен и обычно имеет одну-две кнопки. Подключенный к телефонной линии с вызывающей стороны, BlB обеспечивает бесплатный звонок на этот номер. Пользователь BlB заранее сообщает другим лицам, что они не будут обязаны оплачивать все звонки, сделанные на ЭТОТ номер. Пользователи в этом случае не используют свои устройства для обмана АТС. BlB относительно прост по конструкции (менее сложен чем BB).

Black Box — это резистор (и часто одновременно и конденсатор), помещенный в телефонной розетке вашей линии для того, чтобы оборудование телефонной компании считало, что при входящем звонке вы не взяли трубку и не ответили. В результате тому, кто вам звонил, не будет предъявлен счет за телефонный разговор. Black Box не работает под ESS.

CHEESE BOX

Устройство Cheese Box (далее CB) может быть недоработанным или очень сложным. Размер этого устройства также различен: одно из них было найдено размером в половину одно-долларовой бумажки. CB наиболее часто используется букмекерами или для размещения заработной платы без определения удаленного места, откуда был произведен перевод. CB подключается в 2 телефонных линии, каждая из которых имеет отличный от другой номер, но тем не менее оканчивается в одном и том же месте. В действительности, имеются 2 телефона в одном и том же месте, которые связываются между собой посредством CB. Букмекер, находясь в некотором удаленном местоположении, набирает номер одного из двух телефонов и остается на линии.

Другой пользователь набирает номер другого телефона, но автоматически, посредством CB, связывается с другим телефоном букмекера. Если кроме CB подключен еще и BlB, оборудование АТС разрешает производить еще и бесплатный звонок по другой линии. Если органы правопорядка проводят обыск в месте подключения CB, никакого подвоха не замечается, так как это устройство очень трудно идентифицировать.

RED BOX

Это устройство акустически соединяется с микрофоном трубки таксофона. Устройство излучает сигналы, идентичные сигналам, излучаемым при опускании монеты в монетоприемник. Таким образом, может быть произведен звонок без фактического помещения монеты в монетоприемник.

Когда монета опускается в таксофон, тот испускает набор тоновых сигналов в сторону ACTS (Automated Coin Toll System — система автоматического контроля оплаты разговора). Red Box «обманывает» ACTS, заставляя ее «поверить» в то, что вы поместили монету в аппарат. Red Box просто проигрывает тоны ACTS в микрофон телефона. ACTS принимает эти тоны и позволяет сделать необходимый звонок. Работающие тона:

Сигнал монеты в 5 центов

1700 + 2200 0,060s on

Сигнал монеты в 10 центов

1700 + 2200 0,060s on, 0,060s off, повторить дважды

Сигнал монеты в 25 центов

1700 + 2200 33ms on, 33ms off, повторить 5 раз

Как сделать Red Box

Red Box обычно производятся из различных типов номеронабирателей Radio Shack, открыток фирмы Hallmark или собираются из находящихся под рукой электронных компонентов.

Для того чтобы сделать Red Box из номеронабирателя Radio Shack 43–141 или 43–146, откройте его и замените кварцевый резонатор на новый. Цель этой операции состоит в том, чтобы заставить кнопку (*) вашего номеронабирателя генерировать тон в 1700 Mhz и 2200 Mhz вместо изначального 941 Mhz и 1209 Mhz тона. Точное значение нового резонатора должно быть 6,466806 для создания чистого тона в 1700 Mhz и 6,513698 для тона в 2200 Mhz.

Кристалл с близким значением создаст тон, который может вписаться в рамки допуска ACTS. Чаще всего выбирают кристалл в 6,5536 Mhz, потому что его легко заказать. Старый кристалл — это большая блестящая металлическая деталь, помеченная «3 579545 Mhz». Когда закончите переустановку кристалла, запрограммируйте кнопку P1 на пятикратный набор (*). При нажатии P1 каждый раз будет моделироваться сигнал 25-центовой монеты.

Где можно достать кристалл в 6,5536 Mhz

Проще всего его купить в местном магазине электроники. Кристаллы распространяются компанией Radio Shack, и ваш магазин должен сначала заказать их. На это уйдет приблизительно две недели. Кроме того, многие сотрудники Radio Shack не знают об этой услуге.

Можно заказать кристалл по почте. При этом плата за пересылку и обработку груза намного превысят цену самого кристалла. Самое лучшее собрать знакомых, купить кристалл в складчину и совместно его потом использовать. Или купить пять или шесть кристаллов самому и перепродать их позже. Вот некоторые адреса, по которым можно заказать кристаллы:

Digi-Key

701 Brooks Avenue South

P.O. Box 677

Thief River Falls, MN 56701-0677

(800) 344-4539

Part Number: X415-ND

(Примечание: 6,500 Mhz и только .197 x .433 x .149)

Part Number: X018-ND

JDR Microdevices:

2233 Branham Lane

San Jose, CA 95124

(800) 538-5000

Part Number: 6.5536MHZ

Tandy Express Order Marketing

401 NE 38th Street

Fort Worth, TX 76106

(800) 241-8742

Part Number: 10068625

Alltronics

2300 Zanker Road

San Jose CA 95131

(408) 943-9774 Voice

(408) 943-9776 Fax

(408) 943-0622 BBS

Part Number: 92A057

Mouser

(800) 346-6873

Part Number: 332-1066

Blue Saguaro

P.O. Box 37061

Tucson, AZ 85740

Part Number: 1458b

Unicorn Electronics

10000 Canoga Ave, Unit c-2

Chatsworth, Ca 91311

Phone: 1-800-824-3432

Part Number: CR6.5

Таксофоны, с которыми работает Red Box

Red Box работает с таксофонами компании TelCo и не работает с таксофонами фирмы COCOT.

Как уже говорилось выше, Red Box «надувает» ACTS, заставляя ее «поверить» в то, что разговор уже оплачен. ACTS — программное обеспечение телефонной компании — произносит «Пожалуйста, заплатите столько-то центов» и, слушая, ждет опускание монет.

Таксофоны COCOT не используют ACTS. Модели таксофонов этой фирмы сами контролируют оплату разговоров.

Как позвонить по местному номеру, используя Red Box

Таксофоны не используют ACTS для внутригородских звонков. Для того чтобы использовать вашу Red Box при местном звонке, нужно ввести ACTS в заблуждение относительно месторасположения запрашиваемого номера.

Первый способ это сделать — набрать 10288-xxx-xxxx (в некоторых районах). Это представит ваш разговор как междугородний и приведет к включению ACTS.

В других районах можно позвонить в справочную и узнать телефонный номер нужного вам человека. Оператор продиктует номер, а затем вы услышите примерно такое сообщение: «Ваш звонок может быть автоматически завершен за дополнительные 35 центов». После того, как это случится, вы сможете использовать тона ACTS.

Для чего нужны все эти «цветные коробочки»

Acrylic

Перехват «тройных» звонков, дозвон и программируемая пересылка сообщений на старых 4-проводных системах.

Aqua

Перехват напряжения, используемого ФБР в системах lock-in-trace/trap-trace.

Beige

Телефонная трубка Линемана.

Black

Позволяет тому, кто совершает звонок, избежать предъявления счета за услуги.

Blast

Усилитель телефонного микрофона.

Blotto

Устраивает короткое замыкание для всех телефонов, расположенных в определенном районе.

Blue

Подражает настоящему оператору, перекрывая магистраль с тоном в 2600 hz.

Brown

Создает единую телефонную линию из двух.

Bud

Подсоединение к телефонной линии соседей.

Chartreuse

Использует электричество вашей телефонной линии.

Cheese

Соединяет два телефона для создания дивертера.

Chrome

Манипулирует сигналами дистанционного управления.

Clear

Телефонная спираль датчика и маленький усилитель используются для свободного дозвона с телефонов фирмы Fortress.

Color

Сигнал на линии активизирует телефонный регистратор.

Copper

Устанавливает помехи на расширителе при перекрестной связи.

Crimson

Клавиша «hold».

Dark

Переадресует исходящие или входящие звонки на другой телефон.

Dayglo

Подсоединение к телефонной линии соседей.

Divertor

Переадресует исходящие или входящие звонки на другой телефон.

DLOC

Создает единую телефонную линию из двух.

Gold

Установка маршрута удаленного соединения.

Green

Подражает сигналам «Монета опущена», «Возврат монеты» и ring-back-номеру.

Infinity

Дистанционно активизирует ответвление телефонной линии.

Jack

Touch-tone ключ pad.

Light

Индикатор использования.

Lunch

AM-передатчик.

Magenta

Соединяют одну удаленную телефонную линию с другой.

Mauve

Ответвление телефонной линии без прямого подсоединения.

Neon

Внешний микрофон.

Noise

Создает шумы на линии.

Olive

Внешний звонок.

Party

Создает единую телефонную линию из двух.

Pearl

Генератор звуков.

Pink

Создает единую телефонную линию из двух.

Purle

Телефонная клавиша «hold».

Rainbow

Уничтожает следы пребывания, запуская в телефонную линию 120 v (шутка).

Razz

Подсоединение к телефонной линии соседей.

Red

Дает возможность свободно пользоваться таксофоном, генерируя тон 25-центовой монеты.

Rock

Добавляет музыку на вашу телефонную линию.

Scarlet

Является причиной, по которой телефонная линия соседей некорректно работает.

Silver

Создает DTMF-тоны для A, B, C и D.

Static

Сохранят высокое напряжение на телефонной линии.

Switch

Добавляет возможность сохранения сообщений, огоньки индикаторов, конференц-связь.

Tan

Сигнал на линии активизирует телефонный регистратор.

Tron

Обращают фазу мощности к вашему дому, и ваш электросчетчик крутится медленнее.

TV Cable

«Видит» звуковые волны на вашем TV.

Urine

Создает серьезное нарушение между звонком и каркасом защиты в другой телефонной трубке.

Violrt

Предохранят таксофон от «зависания».

White

Переносная вспомогательная DTMF-клавиатура.

Yellow

Добавляет параллельный телефон.

Часть 3. Модемы и IP-телефония

Модемы: ЧТО ДЕЛАТЬ и КТО ВИНОВАТ?

В повседневной жизни перед человеком, использующим телекоммуникационное оборудование, вопросы, вынесенные в заголовок, встают ежечасно.

- КТО ВИНОВАТ: какие факторы ухудшают качество работы на телефонных каналах;
- ЧТО ДЕЛАТЬ: как можно повысить качество работы на существующих каналах.

Факторы, ухудшающие качество связи по телефонным каналам

Телефонная розетка в вашем доме соединяется с автоматической телефонной станцией двум обычными проводами. По ним в виде сигнала переменного напряжения к вам приходит голос собеседника, по ним же одновременно ваш голос уходит к нему (это дуплексная связь). Для работы микрофона и набора номера по тем же проводам приходит постоянное напряжение. Эти провода обычно называют абонентской линией.

На АТС голоса собеседников разделяются — дифференциальная система преобразует двухпроводную линию в четырехпроводную. Сигнал тональной частоты (ТЧ, диапазон частот 300...3400 Гц, на которых происходит «звуковое» общение) преобразуется в высокочастотный, выполняется частотное уплотнение каналов, далее по одному кабелю передаются сразу несколько разговоров до следующей станции, где голос вернется в звуковой диапазон. Если это не конечный пункт, то снова будет выполнено частотное уплотнение или преобразование в цифровой код, и так до станции, к которой подключен собеседник. Преобразование в высокую частоту и обратно называют участком переприема (ППУ). На базе такой сильно упрощенной схемы рассмотрим, что же ухудшает связь на всех этапах передачи.

АБОНЕНТСКАЯ ЛИНИЯ — многие из них проложены очень давно, в городах кабельные колодцы затопляются водой, в сельской местности это паутины проводов на столбах. Поэтому не приходится удивляться, что именно абонентские линии вносят в сигнал значительную долю искажений:

- затухание (уменьшение мощности) полезного сигнала — одна из самых больших бед абонентских линий;
- перекос амплитудно-частотной характеристики (изменение мощности сигнала в зависимости от частоты) вызван емкостью проводов; естественно, что более высокочастотные сигналы затухают более сильно и, как следствие, на приемнике вызывающего модема (несущая 2400 Гц) сигнал ослаблен сильнее, чем у отвечающего (несущая 1200 Гц);
- импеданс линии (ее комплексное сопротивление); при нормативе 600 Ом ±20% реальные значения доходят до 1800 Ом. Разброс параметров приводит к рассогласованию дифференциальной системы модема и общему снижению его реальной чувствительности;
- постоянное напряжение смещения (то самое, благодаря которому работают микрофоны) может иметь значительные отклонения от номинала; для скоростей обмена до 2400 бит/с этот фактор модемам сильно жизнь не портит, т.к. большинство производителей используют специальные трансформаторы.

УЧАСТКИ ПЕРЕПРИЕМА наибольшее влияние оказывают при междугородней связи, когда их общее число может составлять 8–11 участков. Вносимые искажения во многом зависят от качества настройки полосовых фильтров на телефонных станциях. Основные искажения:

- фазочастотные искажения (отклонение группового времени прохождения относительно его значения на частоте 1900 Гц); переприемы — основной источник этих искажений, возможности модемов по их компенсации обычно ограничены 6–8 участками;
- амплитудно-частотные искажения (затухание на краях полосы пропускания); доля переприемов в общих амплитудных искажениях относительно невелика, кроме случаев встречи с фильтрами, «которых не касалась рука человека»;
- смещение несущей частоты (спектр сигнала равномерно смещается на несколько герц); причина — в

несогласованной настройке генераторов задающих частот аппаратуры уплотнения данных (но за ними обычно следят хозяева каналов), а допуск ±7 Гц, компенсируется модемами; однако приходилось видеть каналы со смещением в 15 Гц;

- джиттер фазы (дрожание фазы по периодическому или случайному закону); в основном вызывается паразитной модуляцией сигнала гармониками питающего напряжения или сигнала вызова (звонка);
- скачки фазы (случайный поток скачкообразных изменений начальной фазы сигнала); возникают при переключениях аппаратуры канального уплотнения.

ПРОЧИЕ НЕПРИЯТНОСТИ, которые могут возникнуть на всем пути сигнала:

- шумы — зашумленность канала оценивается соотношением мощностей полезного сигнала и шумов в полосе канала тоновой частоты; являются одним из основных факторов, ухудшающих качество работы модемов;
- импульсные помехи — случайный поток импульсов напряжения, являющихся причиной плохой работы на многих линиях; источниками помехи могут быть: декадно-шаговое оборудование станций, процесс набора номера на соседних абонентских линиях, изменение напряжения смещения и т.п.;
- замирание сигнала — временное уменьшение мощности сигнала до уровня ниже распознавания модемом;
- колебания амплитуды — периодическое изменение мощности полезного сигнала; измерения позволили обнаружить на некоторых линиях трудно объяснимые низкочастотные колебания в диапазоне 1–10 Гц с амплитудой до 2 дБм;
- ограничение частотного диапазона; кроме рассмотренных выше причин (перекос АЧХ, переприемы), может иметь «рукотворную» природу и производиться персоналом АТС в простейшем случае потому, что абоненты слишком много жаловались на треск в трубке;

- общее ухудшение всех параметров может явиться следствием высокой загрузки каналов связи; по мере ее увеличения подключается более устаревшее оборудование и более низкокачественные каналы.

Характеристики модемов

Обычно производители умалчивают о большинстве параметров, влияющих на качество работы модема, а измерить их без средств оперативной проверки качества работы модемов крайне затруднительно. Часть данных можно найти в каталогах на микросхемы (chipset). Также нужно учитывать, что многие характеристики определяются не только качеством реализации модема, но и ограничениями, накладываемыми стандартами для обеспечения совместимости.

Отдельно необходимо принять во внимание реакцию модемов на дестабилизирующие воздействия, которые приводят к временному искажению информации:

- импульсные помехи с отношением средней мощности сигнала к максимальной мгновенной мощности помехи до -10 дБ;
- временное пропадание входного сигнала до уровня -60 дБм;
- скачки фазы с частотой следования до 15 Гц и амплитудой до 180 град.

Интерес представляет способность модемов к восстановлению работоспособности после окончания этих воздействий. При этом возможны три варианта реакции модема:

- развал внутренних следящих систем и, как следствие, невозможность продолжения сеанса связи;
- обнаружение ситуации и попытка провести процедуру автоматической переустановки соединения (retrain) без разрыва сеанса связи;
- самовосстановление следящих систем без процедуры переустановки, если она в модеме запрещена.

В ситуации отсутствия поддержки процедуры retrain в некоторых типах импортных модемов третий вариант предпочтительнее.

Ощутимое улучшение качества связи может достигаться в модемах, имеющих настройку на конкретную телефонную линию. В рекламных проспектах это свойство иногда называют регулировкой чувстви-

тельности или подстройкой импеданса. Его же физическая природа — в согласовании дифференциальной системы модема с реальной линией. При этом уменьшается мощность выходного сигнала модема, попадающая на вход собственного приемника, что повышает реальную чувствительность к входному сигналу.

Так что же, собственно, делать

Из всех вопросов, с которыми приходится сталкиваться при установке и использовании модемов (сопряжение модема с компьютером, проверка его исправности, установка коммуникационного пакета, работа на «тяжелых» телефонных линиях и специфические вопросы, возникающие при общении с АТС), мы попробуем коснуться лишь тех объективных проблем, которые возникают не вследствие нашего незнания, а ниспосланы нам Свыше.

АТС

Рассмотрим вопросы взаимодействии модема с телефонной станцией. Поскольку телефонная станция не знает кто именно и какими средствами ее (АТС) домогается, модем должен при установке соединения делать все то же самое, что делаете вы, пытаясь дозвониться:

- модем снимает трубку и дожидается сигнала от АТС;
- при обнаружении непрерывного гудка набирает номер и снова ждет сигналов от АТС;
- при коротких гудках вешает трубку, а при длинных ждет когда визави ответит, если же он долго не отвечает — вешает трубку;
- услышав ответ, и разобравшись, что на том конце тот, кто ему нужен, начинает «разговор».

Итак, какие же вопросы могут возникнуть на всех этих этапах?

1. Нет ответов от АТС при снятии трубки, и модем выдает сообщение «NO DIALTONE». Возможны следующие причины (рекомендации по парированию этих неприятностей здесь и далее приводятся после многоточия).

Нарушены электрические цепи между модемом и телефонной линией, или модем неисправен.

... Надо искать неисправность.

Ваш офис подключен к местной АТС типа «Квант» (или аналогичной по принципу работы), а используемый модем имеет оптронную схему набора номера, что нередко встречается в модемах для «notebook» и дешевых изделиях.

... Придется менять тип модема (АТС поменять сложней).

Гудок очень тихий, модем его не слышит.

... Может помочь применение изделий, имеющих программное управление чувствительностью к сигналам АТС или использование команды «AT X1» или «AT X3», разрешающие набирать номер не дожидаясь гудка.

Частотные параметры сигнала АТС сильно отличаются от стандартных.

... Рекомендуется все та же команда «AT X1» или применение адаптированных модемов.

Пожилая АТС не успела ответить за фиксированное время из-за высокой загрузки.

... Придется использовать режим без определения длинного гудка от станции, задавая время от момента снятия трубки до начала набора номера вслепую в регистре S6 модема. Можно также просто не звонить в «час пик» — все равно качество связи будет оставлять желать лучшего.

Разговаривают по параллельному телефону.

... Что делать вы знаете.

Ответа и не должно было быть.

... Вы используете выделенную линию (при этом обычно применяют AT &L1 или AT X1), или АТС настолько своеобразна, что без консультации с связистами не обойтись.

2. Номер набран, но модем не распознает короткие гудки и не выдает сообщение «BUSY». Это доставляет много неудобств, но не является фатальным, т.к. даже не обнаружив сигнала занято модем выдаст сообщение «NO CARRIER» по истечении времени на установление соединения. Рассмотрим возможные причины: — Значительные отличи реальных параметров сигнала от стандартных.

... Желательно применять модемы с расширенными или программно управляемыми диапазонами по частотным параметрам и, что не менее важно, временным соотношениям тон/пауза сигнала «занято».

Взаимное проникновение каналов. На фоне громкого сигнала «занято» тихо, но достаточно для фиксации этого модемом, звучит длинный гудок, предназначенный совсем другому абоненту.

... В таких ситуациях достаточно программно уменьшить чувствительность модема к гудку. — Стоит обратить внимание на строку набора номера. Если она оканчивается «;» и далее идет «AT O», то модем и не должен был распознавать сигнал занято.

3. Удаленный модем снял трубку и отвечает, но ваш модем его не слышит. Если модем исправен и сигнал ответа имеет достаточную мощность, то причина скорее всего в том, что он не смог распознать длинный гудок от АТС перед началом обмена (ваш модем может не уметь одновременно распознавать гудок и сигнал ответа). Это могло произойти, если гудок был очень тихий или очень короткий (встречается на некоторых АТС и многоканальных телефонах).

... Универсальное средство — команда «AT X2».

4. Удаленный модем снял трубку, начал отвечать, но через несколько секунд соединение было разорвано телефонной станцией. Если ситуация повторяется с завидным постоянством, то вам не повезло — где-то на пути сигнала встретилось устаревшее коммутационное оборудование, использующее в качестве команды на разрыв соединения частоту 2100 Гц. Отвечающий модем выдает при установке соединения именно эту частоту.

... Можно предложить два метода борьбы. Перевод отвечающего модема на работу по стандарту Bell 212A (скорость 1200 бит/с), или запрет выдачи этой частоты (вторая возможностью явно реализована всего в несколько типах модемов, в отдельных случаях этот эффект может быть достигнут косвенно, переходом в режим работы на выделенной линии).

ТЕЛЕФОННАЯ ЛИНИЯ

Остановимся на вопросах, возникающих из-за плохого качества телефонного канала. Во многих случаях работу модемов можно улучшить, поняв и измерив происходящее на телефонной линии.

Несколько типов дорогих модемов, а также AnCom ST-2442 позволяют оценить параметры канала. Оперативные средства контроля телефонного канала — тема отдельного рассмотрения, пока же перечислим средства, которые могут помочь улучшить качество связи при поиске вслепую.

1. Стоит всерьез отнестись к вопросу параллельного телефона. Отдельные типы аппаратов (например, кнопочные с запоминанием номера и питанием от телефонной сети) могут значительно испортить телефонную линию даже при положенной трубке.

... Поэтому можно рекомендовать подключать телефонный аппарат только через дополнительный соединитель модема, а также не использовать дешевые модемы, не имеющие такого соединителя или оставляющие его подключенным к телефонной линии при работе.

2. Модемы «MaxCom-2400», «AnCom ST-2442» и некоторые другие имеют средства аппаратной настройки на конкретную телефонную линию, повышающие реальную чувствительность. Настройка зависит только от участка абонент-АТС и поэтому процедура разовая, эффект же от нее на некоторых линиях просто поразителен.

... Попробуйте.

3. Программная регулировка уровня выходного сигнала без специальных средств требует некоторого опыта, т.к. приходится искать компромисс. Повышение уровня улучшает качество приема удаленным модемом, но может ухудшить условия работы собственного приемника. Настройка зависит от типа модема и его согласования с телефонной линией. В качестве средства, облегчающего поиск оптимального уровня можно рекомендовать программы, имеющие индикацию количества сбойных блоков как на прием, так и на выдачу. С некоторыми допущениями их можно использовать в качестве индикаторов качества приема своего и удаленного модемов.

4. Некоторые модемы имеют несколько программных реализаций адаптивных корректоров амплитудных и фазовых искажений. Например: для работы в «нормальных» условиях, на междугородных каналах (большое количество участков переприема) и сельских линиях (большое затухание и перекос АЧХ).

5. На линиях с очень высоким уровнем шумов можно встретиться с курьезными ситуациями. На них успешно работают очень дорогие, а также очень простые и дешевые (поддерживающие только скорость 1200 бит/с) модемы. Основная же масса изделий функционирует из рук вон плохо.

... Объяснять почему работают дорогие модемы не надо, на то они и дорогие. Для всех остальных ситуация складывается следующим образом. В модемах, работающих на скорости 2400 бит/с, для компенсации искажений телефонного канала реализуется алгоритм адаптивного корректора. В момент начальной настройки он достаточно чувствителен к уровню шумов и при их высоком уровне может произвести неправильную установку, ухудшающую качество работы. В этих модемах адаптивный корректор не отключается и на скорости 1200 бит/с, где его работа не является обязательной, поэтому понижение скорости не приносит ожидаемого улучшения. Модемы, поддерживающие только скорость 1200 бит/с, адаптивного корректора не имеют вовсе и сами себе жизни не портят. Так как низкоскоростные модемы для большинства применений уже морально уста-

рели, можно считать оптимальным использование изделий, имеющих возможность программного отключения адаптивного корректора для скорости 1200 бит/с.

6. Непосредственно при установке соединения некоторую помощь может оказать изменение значения регистра S9. Его увеличение помогает отсечь шумы, характерные для момента установления соединения, которые могут ошибочно приниматься за несущую удаленного модема. Чрезмерно увеличивать это значение не нужно, чтобы не пропустить самой несущей.

7. Соединение успешно установлено, вы обмениваетесь данными, но периодически связь разрывается или появляется «мусор» на экране (при соединении без коррекции ошибок).

... Не вдаваясь в причины на физическом уровне (большое затухание, импульсные помехи, периодическое замирание сигнала и т.п.), во многих случаях поможет увеличение значения регистра S10. В нем программируется задержка между обнаружением модемом пропадания сигнала от удаленного модема и моментом, когда он вешает трубку, выдавая сообщение «NO CARRIER». Для некоторых коммуникационных пакетов при этом желательно выдать команду «AT &C0», запрещающую отображать потерю несущей от удаленного модема в бите DCD коммуникационного порта.

МОДЕМЫ

Иногда причиной отказов могут быть сами модемы. Если обмен данными или процесс установки соединения неожиданно «зависают», стоит внимательно рассмотреть используемые модемы. Возможно, причина в том, что в одном из модемов программно выключена или просто не реализована процедура retrain. При ухудшении качества связи модем, поддерживающий retrain, пытается его выполнить. Но не находит понимания у партнера — процесс зацикливается. Избежать «зависаний» можно при разрешении или запрещении процедуры одновременно на двух модемах.

HOST

Особняком стоят вопросы, специфичные для работы модема в режиме автоматического ответа.

Устойчивое определение телефонного звонка от АТС зависит от аппаратуры модема. Встречаются телефонные станции, формирующие очень слабые сигналы, не обнаруживаемые модемами без средств адаптации.

Паразитная фиксация телефонного звонка при наборе номера на параллельном или подключенном через соединитель модема телефоне

зависит как от модема, так и от коммуникационного обеспечения. Алгоритмическая обработка позволяет модему выделить сигнал звонка (правда реализовать эту возможность удосужились далеко не все производители). Часть программных пакетов фиксирует сигнал звонка непосредственно в интерфейсе с компьютером (а не по сообщениям «RING»), что во многих случаях сводит на нет обработку в модеме. Аналогичные проблемы могут возникнуть при использовании спаренных телефонов.

Неприятности возникают при разрыве соединения, если абонент грубо вешает трубку на своем модеме, не выдав на host команды окончания сеанса. Модем, находящийся в режиме автоматического ответа, может на фоне гудков от станции принять свой собственный выходной сигнал за несущую от удаленного модема и заблокировать дальнейшую работу.

... Методов борьбы несколько: уменьшение мощности выходного сигнала, уменьшение значения регистра S10, ну и конечно применение качественных модемов.

Одновременная передача голоса и данных через канал тональной частоты

Последнее время очень популярной считается тема передачи голоса через Интернет. Эта необходимость может возникнуть, например, в медицине, когда необходимо пояснять выводимую на экран информацию, а также во многих других областях, где требуется вмешательство голоса.

Существуют два конкурирующих между собой основных стандарта. Первый связан с аналоговой передачей голоса и данных (Analog Simultaneous Voice/Data — ASVD), когда данные и звук передаются по отдельным каналам. Второй способ предполагает цифровую передачу голоса вместе с данными (Digital Simultaneous Voice/Data — DSVD). По методу DSVD голос оцифровывается, мультиплексируется с данными и передается в едином потоке. DSVD стандартизирован ITU и описан в рекомендации V.70.

ASVD (рекомендация ITU — V.61) обрабатывает голос, данные, и информацию управления как раздельные объекты. Пользователю, это обеспечивает некоторый комфорт, потому что голос не цифровой. Однако, чтобы обеспечить передачу всех трех каналов, речевая ширина полосы частот ограничивается 2400 Hz и ширина полосы частот данных ограничивается скоростью 4800 бит/сек.

DSVD (рекомендация ITU — V.70) обрабатывает всю информацию которую он получает как цифровую. Речевым пакетам дан приоритет над пакетам данных, но они передаются через ту же самую схему как и данные. Ничего не делается для того, чтобы увеличивать скорости передачи данных, обнаружив паузу. Скорость передачи данных увеличивается только за счет использования протоколов сжатия модема. Он позволяет передавать данные на скорости до 28.8 кбит/с.

Каждая из этих технологий выполняется через режим, который позволяет модему инициализировать режим SVD без приостановки интерактивного соединения. Оба типа модема вызываются телефоном. Когда пользователь поднимает трубку модем пробует установить SVD сеанс с другим модемом. Если удаленный пользователь отвечает поднимая трубку удаленного модема, тогда SVD сеанс устанавливается.

DSVD имеет большое количество технических и практических преимуществ, в то время как ASVD имеет одно, но наиболее существенное преимущество, касающееся качества передаваемой речи.

А теперь вашему вниманию хотелось бы предложить еще одно из решений поставленной выше проблемы, одновременной передачи данных и голоса — это передача голоса отдельно от передачи данных в неиспользуемой полосе частот. Поясним это более конкретно. Каналу тональной частоты доступна полоса частот шириной 3100 Гц (от 300 до 3400 Гц), а модемы же, использующие стандартные протоколы передачи данных V.21, V.22, V.22bis...V.32bis, работают в полосе частот, максимально, от 600 до 3000 Гц, оставляя неиспользуемым полосы частот от 300 до 600 Гц и от 3000 до 3400 Гц. Это же относится к некоторым нестандартным протоколам, таким как V.32terbo, HST, ZyX для скоростей до 16800 бит/с. Это не использование связано с завалами частотной характеристики по краям канала ТЧ. В протоколах V.34 и PEP(Turbo PEP) используется вся полоса канала ТЧ, поэтому их исключим из дальнейшего рассмотрения.

Таким образом, мы имеем свободную полосу частот шириной 700 Гц, что не достаточно для передачи речи, но вполне достаточно для передачи сжатой речи.

Передаваемая речь не будет влиять на скорость передачи данных (так как она она будет передаваться независимо), то есть скорость модема будет достигать, максимально, 19200 бит/с без учета компрессии. Доработок модем не требует, а необходимо только лишь создать устройство преобразования речи.

Процесс установления соединения можно представить следующим: при поднятии трубки посылается вызов противоположной стороне

на частоте не входящей в полосу передачи модема (в этот момент модемы передают данные). С той стороны поднимается трубка и, таким образом, устанавливается соединение. Отбой происходит аналогично.

В принципе возможны два способа сжатия речи — непосредственное и параметрическое. Если рассматривать это применительно к частотному сжатию под непосредственным понимается такой способ, при котором компрессия частотного диапазона осуществляется путем непосредственного преобразования спектра без какого-либо его анализа и разложения, а восстановление происходит без применения местных источников сигналов. А параметрическим сжатием называют такой способ преобразования сигнала, при котором его компрессия осуществляется путем выделения из него ограниченного числа медленно меняющихся параметров, по которым сигнал может быть восстановлен, а восстановление производится за счет местных источников, управляемых этим комплексом параметров. Таким образом, при частотном параметрическом сжатии в канал поступает не сам спектр речи, а только лишь сведения об его характерных особенностях (параметрах). Восстановление исходного спектра осуществляется путем воздействия этих сигналов на равномерный спектр, созданный местным генератором, моделирующим те особенности речевого сигнала, сведения о которых не нужно передавать через канал.

Устройства для параметрического частотного сжатия речи получили название вокодеров (англ. voice coder — кодировщик голоса). В зависимости от принятой системы параметров, по которым производится восстановление первообразного речевого сигнала. Различают основные типы вокодеров: полосные, форматные, гармонические.

Главными частями вокодерного тракта является анализатор, который осуществляющий выделение параметров речевого сигнала, система передачи, обеспечивающая прохождение информации об этих параметрах через канал связи в узкой полосе частот, и синтезатор, восстанавливающий первообразный речевой сигнал.

Анализатор вокодера состоит из устройства для выделения параметров речевого сигнала A1,A2,...,Ak и схемы выделения основного тона (тон (F0) или шум).

Полосовой вокодер

В полосном вокодере параметрами, описывающими текущий спектр, являются средние уровни энергии речи в полосах, на которые делится частотный диапазон.

Анализатор полосного вокодера состоит из схемы выделения ОТ и устройства для выделения параметров огибающей спектра. Последнее представляет собой совокупность некоторого числа (от 10 до 20) спектральных каналов, в которых производится определение среднего уровня речи. Чем больше будет взято число таких каналов, тем большая будет достигнута точность аппроксимации спектра, но тем меньшим будет коэффициент компрессии.

Погрешность преобразования связана с тем, что реальная огибающая речевого спектра заменена здесь ступенчатой функцией. Степень приближения последней к реальной кривой зависит от числа спектральных каналов.

Полосные вокодеры обеспечивают высокую разборчивость речи (до 85% разборчивости слогов), но натуральность ее, как и в других системах вокодеров, значительно снижается.

Форматный вокодер

В форматных вокодерах восстановление речевого сигнала производится по информации о форматных максимумах. Параметрами, передаваемыми по каналу связи и позволяющими с достаточным приближением синтезировать картину текущего спектра, являются здесь сигналы о средних частотах и уровнях: формант.

Устройство для выделения параметров в анализаторе вокодера состоит из трех каналов, выделяемых с помощью трех широкополосных фильтров ПФ1–ПФ3. Взаимно-перекрывающиеся полосы пропускания этих фильтров соответствуют областям, в которых могут находиться три возможные форманты речевых звуков. На выходе каждого фильтра включено устройство, определяющее частоту и уровень форманты.

В случае форматного вокодера необходимо передать всего 7 параметров.

Форматные вокодеры способны обеспечить больший коэффициент компрессии, чем полосные, но имеют несколько пониженное качество синтезируемой речи (65%).

Гармонический вокодер

В 1958 году А. А. Пироговым был предложен еще один способ построения вокодера, в основе которого лежит гармонический анализ мгновенного спектра, т. е. разложение его огибающей в ряд Фурье с последующей передачей на приемный конец информации о коэффициентах этого ряда.

При использовании вокодеров можно получить достаточно хорошее сжатие речи. Но к сожалению эта речь будет страдать не натуральностью, поэтому использование этого метода передачи данных и голоса не будет рекомендоваться для коммерческого использования, а только для ведения служебных переговоров. Кроме того, использование крайних участков канала ТЧ заставляет использовать достаточно сложные системы для восстановления принятой информации, так как края канала ТЧ, как говорилось выше подвержены значительным амплитудно-частотным искажениям. А это значит, что данная система все еще требует работы и работы...

История развития протоколов передачи данных

С каждым годом растет количество передаваемой информации, ширится сеть Интернет, растут предоставляемые услуги по использованию средств связи, появляются новые технологии, а что же происходит в России с ее огромными просторами и, доставшейся в наследство от СССР, устаревшей инфраструктурой кабельных сетей и связного оборудования.

После выхода протокола V.32 bis в нашей стране появились модемы обеспечивающие максимальную скорость 14400 бит/с. Были приобретены модемы поддерживающие данный протокол. Это были Unicom 1414 VQE, USRobotics, ZyXEL. Кроме этого протокола последние содержали и фирменные, такие как HST и ZyX. Перечисленные выше модемы позволяли работать со скоростями до 14400–16800 бит/с, но в реальности скорость передачи данных редко превышала 4800–9600 бит/с. Таким образом, возник вопрос: «Почему?» И начались попытки выяснения причин влияющих на скорость и качество передачи данных.

Первые протоколы имели низкую скорость передачи данных, что обуславливалось, тем, что в пору их создания существующие телефонные сети обладали рядом характеристик, которые не позволяли передавать по ним информацию с большей скоростью. Оборудование, используемое на сетях связи, в большинстве своем было аналоговое, что вносило следующие негативные характеристики:

- ограничение полосы пропускания канала. Эта характеристика связана с завалами частоты на краях канала, кроме того, его ширина могла значительно уменьшится при неоднократном прохождении через участки НЧ (низко-частотный) переприема. Этот

параметр характерен для каналообразующей аппаратуры с частотным разделением каналов (ЧРК), в частности К-60П. Стандартно канал ТЧ имеет полосу пропускания от 300 до 3400 Гц. При 12 транзитных участках с аппаратурой К-60П эффективно передаваемая полоса сужается до пределов 450–2850 Гц.

- сдвиг частоты. Он вызывается отсутствием синхронизма между задающими генераторами в оконечных устройствах аппаратуры с ЧРК.
- неравномерность группового времени прохождения (ГВП). Это проявляется в виде неодновременности прихода боковых полос к приемнику, что препятствует восстановлению сигнала.
- импульсные помехи. Они могут быть связаны с коммутационным оборудованием, перекрестными наводками от вызывных импульсных токов.
- перерывы связи. Они вызываются плохими контактами в разъемах, реле, искателях, что характерно для декадно-шаговых автоматических телефонных станций (АТСДШ).

В связи с перечисленным выше первые протоколы разрабатывались для ограниченной полосы частот на которой такие мешающие факторы, как ГВП и сужение полосы пропускания, не оказывали значительного влияния. В качестве вида модуляции использовалась частотная и фазоразностная. В качестве протоколов использующих этот вид модуляции можно привести V.21–V.27, а также протоколы AT&T. Так как на выделенных каналах не используется коммутация, то и качество передаваемой информации на них значительно превосходит коммутируемую сеть, так и появился протокол V.29, который использует квадратурную амплитудную модуляцию и большую, нежели низшие протоколы полосу частот.

Время шло, шло развитие коммутационного и каналообразующего оборудования, а также развитие микропроцессоров, как следствие улучшаются характеристики каналов связи, а значит появляется возможность создания более высокоскоростных модемов. Но замена каналообразующего оборудования происходила не в один момент, и поэтому выпуск более скоростных протоколов, таких как V.33 для выделенных каналов и V.32, V.32 bis для ТфОП, был нацелен все еще на то, чтобы использовать не всю возможную полосу частот каналов ТЧ, а только ее часть — от 600 до 3000 Гц. Этим страдали и другие фирменные протоколы:

- Express 96 «Ping Pong Protocol». Этот протокол появился в модемах Hayes в 1987 году марки Smartmodem 9600. Модем использовал частный протокол модуляции, называемый Express 96 (также известный как Hayes «Ping Pong Protocol»). По своей сути он был близок к V.32. На сегодняшний день он не используется.
- CompuCom CSP. В то время, когда каждый изготовитель модема переходил на V.32, компания CompuCom в 1991 году выпустила модем SpeedModem Champ. Это был модем со скоростью 9600 бит/с с частным протоколом модуляции, называемым CSP. SpeedModem Champ был модемом с частным протоколом, который стоит меньше, чем модем с V.32. CompuCom распалась в 1992 году.
- HST. Протокол HST разработан фирмой U.S.Robotics и реализован в модемах фирмы серии Courier в 1989 году.

Исключение составляли лишь полудуплексные протоколы семейства PEP разработаны фирмой Telebit и реализованы в модемах фирмы серий TrailBlazer (PEP) и WorldBlazer (TurboPEP), начиная с 1985 года, которые в 1988 году достигли скорости 19200 бит/с, а в последствии и 23000 бит/с. Они пытались использовать всю возможную полосу каналов ТЧ и показывали неплохое качество работы и высокие скорости передачи данных. Но, к сожалению, были они достаточно дороги и закрыты, что сказалось на их распространении и конечно же на скорости. Поэтому организация где я работал не могла позволить себе купить подобную аппаратуру, а обходилась более дешевыми моделями модемов.

Но не все оказалось так плохо. Длительное измерение выделенных каналов, приведение их параметров в норму значительно изменило положение вещей. В ряде случаев произошло повышение скоростей работы аппаратуры передачи данных, а в большинстве своем мало, что изменилось, и спустя время выяснилось почему — в наших бедах оказались виновными прямые провода, которые шли от МТС к конечным пользователям и ложная уверенность их в том, что чем выше уровень передаваемого сигнала, тем лучше. Это хорошо проходило с прямыми проводами, но было не допустимо для аналоговых систем передачи.

Это были проблемы междугородних выделенных каналов, а вот дела с коммутируемой сетью обстояли значительно хуже. Установление соединения в этом случае происходит каждом по разному, конечно, если не используется внутристанционное соединение, и найти участок который виновен в низкой скорости не представляется возможным, тем более, что на ТфОП до сих пор преобладают механические АТС, и немалую часть занимают АТСДШ. Для этих АТС характерны перерывы связи, из-

за быстрого износа скользящих контактов, а также нарушение контактов из-за вибрации стоек, связанной с установлением соединения. На ЦСДО «Искра-2» системы типа АТСДШ отсутствуют, поэтому наблюдаются значительно лучшее качество и более высокие скорости.

Таким образом повлиять на коммутируемые сети было не возможно и поэтому все внимание было уделено выделенным междугородним каналам. «Вылизывание» каналов дало свои плоды, и со временем скорости аппаратуры передачи данных уже редко опускались ниже 14400–9600 бит/с, но требовалось большее. Эти скорости уже не удовлетворяли конечных пользователей, при этом учтите, при передаче данных использовался синхронный режим при котором нельзя было воспользоваться как протоколами сжатия, так и протоколами коррекции ошибок. Потребности росли. Появилась необходимость передавать одновременно данные и голос. Таким образом, мы перешли к другому типу передачи информации.

Одновременная передача данных и голоса

Существует еще одно направление в разработке протоколов передачи данных — это одновременная передачи данных и голоса, которая бывает просто необходима, например, при работе врачей и людей других специальностей, при работе которых необходим одновременный обмен данных и голоса. Работы в данном направлении велись начиная с 60-х годов. Как было сказано раньше, характеристики каналов в то время, да и техника не позволяли работать аппаратуре передачи данных с высокими скоростями, поэтому в качестве речепреобразующих устройств использовались вокодеры: форматный и полосовой, которым было достаточно скорости 1200–2400 бит/с. Передача речи шла, либо в ущерб передачи данным, то есть она прерывала последнюю, либо совместно, то есть на каждую из передач выделялась полоса, в которой они и велись. Речь получалась синтезированная, из чего следовала плохая разборчивость — ниже 90%, и плохая узнаваемость. С подобной техникой автору пришлось работать, так что он знаком с ней не понаслышке. Данные системы не получили коммерческого развития, а использовались в основном для служебных переговоров, либо в спецаппаратуре.

Первые протоколы, реализующие подобную услугу для коммерческого использования, появились в начале 90-х. В качестве примера могу привести протокол MSP Multi-Tech System. Чем же отличаются способы объединения речи и данных?

Протокол ASVD, например V.61, обрабатывает голос, данные, и информацию управления как раздельные объекты. Пользователю, это обеспечивает некоторый комфорт, потому что голос не цифровой.

Протокол DSVD, например V.70, обрабатывает всю информацию, которую он получает как цифровую. Речевым пакетам дан приоритет над пакетам данных, но они передаются через ту же самую схему как и данные. Ничего не делается для того, чтобы увеличивать скорости передачи данных, обнаружив паузу. Скорость передачи данных увеличивается только за счет использования протоколов сжатия модема.

Но подобные нововведения требуют достаточно высокой скорости и качества передаваемых данных, что редко обеспечивалось на практике. Таким образом, назрела необходимость введения нового протокола передачи данных.

Появление V.34

Необходимость в высоких скоростях передачи данных заставила разработать и выпустить на рынок следующие протоколы: HST, ZyX, V.32terbo со скоростями от 16800 до 19200 бит/с. Они разрабатывались на основе протокола V.32bis. Но и этих скоростей стало не хватать. Различные компании начинают разработку модема, работающего со скоростью 28800 бит/с — V.fast. И в 1996 году был объявлено о выходе V.34, который включал в себя различные технологии запатентованные 17 компаниями. Этот протокол в отличии от предшествующих, за исключением PEP и TurboPEP, использует всю ширину аналогового канала. Это и многое другое позволяет ему работать на скоростях до 33600 бит/с по аналоговому каналу, но работа модема на максимальной скорости не возможна через аппаратуру с ЧРК, так как происходит выход за пределы канала ТЧ, поэтому максимальная скорость для канала ТЧ составляет 31200 бит/с, что тоже не плохо. Этот протокол явился последним аналоговым протоколом передачи данных.

Исследования установили, что на качество передаваемой информации влияют следующие характеристики каналов ТЧ — это перерывы связи, скачки фазы, амплитуды, импульсные помехи. Кроме того, было выявлено, что использование нового протокола (V.34) на малых скоростях (до 9600 бит/с) не выгодно. Его рекомендуется использовать лишь на более высоких скоростях. Таким образом, результаты проведенных многолетних исследований позволили создать некоторую методику, следуя которой можно было повысить качество передаваемой информации.

Время не стоит на месте. В начале 1997 года появились модемы, работающие со скоростями до 56700 бит/с по протоколам X2 (3Com-USRobotics) и K56Flex (Lucent Technologies (AT&T), Motorola, Rockwell), а осенью 1998 года был принят протокол V.90 ITU, включающий в себя 11 пунктов из стандарта K56Flex и 1 пункт из X2. Эти модемы предназначены для работ с цифровыми АТС. Идущий к абоненту поток может пе-

редаваться со скоростями до 56700 бит/с, а от него на скоростях до 33600 бит/с, то есть по V.34. Этот протокол используют ИКМ (импульсно-кодовая модуляция) и обеспечивают взаимодействие аналоговых и цифровых сетей. Так как скорости первичного канала ЦСП (цифровой системы передачи) составляют 32, 40, 64 Кбит/с, то протокол V.90 обеспечивают непрерывность передачи данных.

Что же это дало для конечного пользователя? Прежде всего это позволило полноценно работать с Интернетом, ведь в данной сети больше информации идет к пользователю, а от него лишь команды управления. Но эти преимущества получило меньшинство, так как я уже писал выше, в России преобладают электромеханические АТС и аналоговые каналы связи, так что повышение скорости мало сказалось на повышении производительности. Максимальная скорость возможная на канале ТЧ не превышает 3100 бит/с. Это связано с тем, что в реальности протокол V.34 пытается использовать большую полосу частот, чем позволяет канал ТЧ. В этом случае на помощь приходят протоколы сжатия и коррекции ошибок.

Протоколы коррекции ошибок и сжатия

Одновременно с развитием протоколов передачи данных шло и развитие протоколов сжатия коррекции ошибок. Это было связано с тем, что требовалась передача больших объемов информации, чем позволяли существующие модемы, кроме того, как было сказано выше, качество каналов обещало желать лучшего. Поэтому фирмы — производители модемов разрабатывали для своей аппаратуры передачи данных необходимые ей протоколы сжатия и коррекции ошибок. Несомненно, лучшими среди них являются V.42 и V.42bis, которые вобрали в себя лучшее из появившихся ранее протоколов.

Сотовые сети связи

Появление сотовых сетей заставило разрабатывать специальные протоколы для них, так как этот вид сетей отличается от сети общего пользования тем, что имеет совершенно другую среду распространения — радиоволны. Таким образом, системы сотовой связи имеют свои специфические проблемы при передаче данных. Например, происходит разрушение данных в результате кратковременных сбоев передачи, когда система сотовой связи переключает вызовы с одной частоты на другую, чтобы избежать наложения с вызовами на ближайших частотах или перейти на освободившийся канал более высокого качества.

Кроме того, возможно разрушение данных, вызванное затуханием сотового сигнала, что происходит довольно часто. Поэтому редко удается работать со скоростями выше 9600 бит/с. В связи этим были разработаны специальные протоколы: MNP10, ETC, HST, ZyCELL.

Протокол ETC работает совместно с V.32bis и V.42. Он позволяет осуществлять контроль за амплитудой передаваемого сигнала, автоматически изменяет скорость соединения в зависимости от состояния канала (уменьшение отношения сигнал/шум, колебания фазы), допускает переход в режим более ранних стандартов, таких как V.22 со скоростью 1200 бит/с, если канал связи не в состоянии обеспечить даже 4800 бит/с, обеспечивает быстрый запуск, использует меньший размер кадра, 32 байта вместо 128 байт, имеет возможность селективного отказа, делает до 20 попыток повторно послать кадр, куда вкралась ошибка.

Стабильность работы протокола MNP10 достигается за счет многократного повторения попытки установить связь, изменения размера пакетов и даже динамического изменения протокола соединения в зависимости от качества канала связи.

ZyCELL автоматически меняет скорость в зависимости от характеристик канала, при переходе из одной ячейки в другую от 0,2 до 1,2 с не прерывает связь и быстро синхронизируется, изменяет уровень сигнала.

Но, к сожалению, встает вопрос о реальной скорости передаче данных по сотовой сети. А это порядка 4800 бит/с, что сегодня недостаточно. С начала 1998 года МСЭ поставил своей целью разработать стандарт для сотовых систем нового поколения, который получил название UMTS. Этот стандарт позволит пользователям увеличить многократно скорость обмена информацией. В частности 144 Мбит/с для быстро перемещающихся абонентов, 384 Мбит/с для пешеходов, 2 Мбит/с для фиксированных терминалов.

Новые протоколы и их возможности

8 Июня 2000 года появилось сообщение о появлении целой серии новых протоколов для передачи данных по ТфОП. Это протоколы V.92, V.44, V.59. А в ноябре они стали официальными. Чем же они отличаются от своих предшественников?

Начнем рассмотрение с V.92, который позволяет увеличить максимальную исходящую скорость от пользователя с 33,6 (V.90) до 48 Кбит/с. Это достигается за счет изменения способа кодирования информации. Теперь оно осуществляется с помощью ИКМ (импульсно-кодовая модуляция). Но ее применение заставляет придерживаться более жестких требований в отношении оборудования, находящегося на пути следования передаваемой информации — должно быть не более чем одно аналого-цифровое преобразование. Исходящая от пользователя

информация может передаваться со скоростями от 24 до 48 Кбит/с с шагом 1,333 Кбит/с как и в протоколе V.90. Кроме того, уменьшается время вхождения в связь с 20 (V.90) до 10 с.

Второй протокол V.44 позволяет увеличить степень сжатия передаваемых данных как 6:1, то есть на 25% в сравнении с V.42bis, который обеспечивал сжатие 4:1. То есть производительность сможет увеличиться до 300 Кбит/с. Но это преимущество не удастся испытать тем, кто использует последовательный порт компьютера, скорость которого ограничена и составляет 115,2 Кбит/с. В качестве алгоритма сжатия используется LZJH, разработанных US-based Hughes Network System.

И, наконец, третий протокол V.59 вводит такую услугу, как возможность прерывания передачи данных на время от 0 до 16 минут и ответ входящему вызову.

Введение данных протоколов, тем более что многие фирмы производители модемов поддержали их, позволит пользователям более активно работать с аудио и видео информацией. Но к сожалению, те кто не мог соединяться по протоколу V.90 не получат ничего. Да и те, кто работает с модемами через последовательный порт с максимальной скоростью 115200 бит/с тоже вряд ли смогут насладиться высокими скоростями.

Кабельные Модемы

Столкнувшись с неудовлетворительной работой сетевых служб, пользователи первым делом обращаются к провайдеру с требованием решить проблему. В случае многих и многих служб на базе Интернета, наиболее очевидным узким местом является «последняя миля», т. е. абонентская линия, по которой дома, отели и небольшие компании подключаются к ближайшей точке доступа в высокоскоростную сеть провайдера. Результатом его наличия становится неудовлетворенный спрос, а то и прямое недовольство пользователей неспособностью владельцев кабельных сетей и местных операторов связи предоставить услуги в 1 Мбит/с или более быстрые, хотя рекламные буклеты обещают их по крайней мере с 1993 года. Несмотря на циничные отказы некоторых провайдеров услуг реальные причины задержки имеют технический и финансовый характер и должны быть устранены прежде, чем пользователи смогут начать искать себе новый повод для огорчений.

Три главных претендента на предоставление широкополосных информационных услуг за пределами офисных зданий и промышленных зон — кабельные модемы, асимметричная цифровая абонентская линия (Asymmetric Digital Subscriber Line, ADSL) и та или иная форма беспроводной связи (радиоволны способны достигать практически любой точки). Эти три технологии отличаются друг от друга пропускной способностью, архитектурой, надежностью защиты и управляемостью. Данными различиями, в свою очередь, определяются накладные расходы для сервис-провайдеров и стоимость услуг для абонентов. С учетом всех названных факторов, доступные абонентам виды услуг могут кардинальным образом отличаться друг от друга.

Кабельная сеть

Кабельное телевидение появилось как способ доставки десятков, а затем сотен аналоговых видеоканалов на 6 МГц в квартиры и дома. С технической точки зрения выделить канал на 6 МГц для цифровых данных и с помощью известных методов модуляции передавать их со скоростью 30 Мбит/с по коаксиальному кабелю не составляет труда. (Общий диапазон рабочих частот коаксиального кабеля близок к 1 ГГц.) Канал на 20 Мбит/с способен поддерживать любую мыслимую информационную услугу, и при этом еще останется место для поддержки видеоконференций и одного-двух каналов видео по запросу. Однако на практике пропускная способность кабельных информационных систем ограничена 10 Мбит/с ввиду использования ими интерфейсов Ethernet.

Применение систем кабельного ТВ для интерактивного обмена данными осложняют следующие два архитектурных вопроса. Во-первых, в большинстве своем они предназначены для передачи сигналов только в одном направлении, а во-вторых, используются обычно совместно десятками, а то и сотнями пользователей в одном доме.

Бум сетей кабельного ТВ в Америке пришелся на 80-е годы. Однако только после 1990 года операторы КТВ стали устанавливать усилители для разделения используемого диапазона частот кабеля на два — прямой и обратный, чтобы обратный трафик не блокировался ранее установленными однонаправленными усилителями. Такие усилители необходимо размещать через каждые полкилометра, или даже чаще, так что подобная задача оказывается весьма непростой.

Кроме того, сети кабельного ТВ и, в частности, частотный диапазон между 5 МГц и 42 МГц, выделенный для обратных информационных каналов, чрезвычайно чувствительны к внешним помехам со стороны радиопередатчиков, бытовых приборов и регуляторов освещенности. Усилители обратного трафика вместе с сигналом усиливают и шум, так что иерархическая «шинная» топология способствует концентрации шумов по мере приближения сигнала к распределительному устройству.

Некоторые операторы КТВ просто отступили перед таким количеством проблем организации обратного потока и устанавливают ка-

бельные модемы со встроенными аналоговыми модемами для передачи обратного трафика по обычным коммутируемым телефонным линиям. Но такое решение увеличивает общую стоимость, вносит обычную задержку на ожидание ответа модема на другом конце и ограничивает максимальную скорость прямого канала (в общем случае, подтверждениям TCP о приеме требуется обычно 10% от пропускной способности прямого соединения; таким образом, прямой поток не может быть больше 288 Кбит/с, если обратный представляет собой модемное соединение на 28,8 Кбит/с). Однако данное решение может рассматриваться только в качестве временной меры. Для пользователей оно имеет целый ряд неудобств.

Для работы в Интернете им по-прежнему нужна будет телефонная линия, а это не может не вызывать недовольство других домочадцев. Кроме того, им придется ждать какое-то время, пока будет установлено модемное соединение, тем самым они лишатся такого преимущества использования кабельных модемов, как мгновенный доступ. Наконец, это решение недостаточно или вообще непригодно для симметричных приложений — ICQ, видеоконференции и т. п. Использование обратной телефонной линии может причинять неудобства и самому оператору. Это и усложнение конфигурации системы, и необходимость выделения двух портов маршрутизатора для одного клиента, и усложнение диагностирования и поддержки системы.

Вместе с тем внешние шумы (шумы ингрессии) ограничивают пропускную способность обратного канала рамками 200–2000 Кбит/с.

Опасность представляют:

- небрежно инсталлированные или корродированные домовые и распределительные разъемы;
- абонентские кабели низкого качества;
- абонентские терминалы;
- прокладка кабеля самими абонентами;
- поврежденный распределительный кабель;
- поврежденное распределительное оборудование, недостаточно надежное заземление системы.

Основными источниками шумов ингрессии являются:

- системы радиокоммуникаций;
- электромоторы;

- переключатели;
- выключатели;
- высоковольтные линии передач;
- электростатические разряды.

Наиболее широко используемый метод модуляции, Quadrature Phase Shift Keying (QPSK), недостаточно эффективен, но его применение зачастую неизбежно, ввиду высокой зашумленности. QPSK модуляция теоретически обеспечивает эффективность использования канала 2 Мбит/Гц. Так как шум создает помехи передаче данных, то необходимо устранить его влияние. Механизм, используемый для этой цели, называется канальным кодированием FEC (forward error correction). Так как канальное кодирование предполагает избыточность, то на него тратится часть пропускной способности, и скорость передачи полезных данных ниже эффективности канала. Механизмы канального кодирования и требования к избыточности в разных системах СКМ различны. СКМ, использующие QPSK, обычно обеспечивают эффективность передачи полезной информации от 1.5 до 1.8 Мбит/Гц.

Одна из наиболее неприятных особенностей шумов ингрессии — случайный характер их появления. Это значит, что и в тех случаях, когда удается обнаружить чистый участок спектра при установке СКМ, нет гарантии, что шумы ингрессии не поразят этот участок позже. В этом случае может быть поврежден канал передачи данных и даже полностью нарушена связь. Шумы ингрессии могут негативно влиять даже на СКМ с мощным канальным кодированием, так как корректирующие возможности любой системы все же ограничены. Единственный способ избежать разрушающего действия этих шумов заключается в перемещении канала связи на чистый участок спектра. Эта способность СКМ называется механизмом уклонения от шумов ингрессии, или частотной отстройкой (frequency hoping). СКМ с частотной отстройкой обладает гораздо большей устойчивостью к разрушению канала во время появления шумов ингрессии.

Во избежание конфликтов в общем кабеле, доступ каждого узла требуется контролировать в обратном направлении. В большинстве случаев операторы КТВ используют механизмы контроля доступа к среде с подачей команд о выделении пользовательской системе квантов времени для передачи трафика.

Другие методы устранения шума:

- Фильтр блокировки шума, управляемый кабельным модемом. Фильтр представляет собой прибор,

блокирующий сигналы обратного канала все время, за исключением моментов передачи данных. Фильтр обычно устанавливается около абонентского ответвителя и предохраняет от шумов ингрессии, наводимых через абонентский отвод или из квартиры абонента.

- Комбайнер обратного канала. Комбайнер обратного канала представляет собой многопортовый переключатель радиосигналов, способный объединять несколько обратных каналов в единый поток, не накапливая при этом шум из индивидуальных обратных каналов. Для этого можно использовать и пассивный комбайнер, однако такое решение не позволяет объединять более 4 индивидуальных каналов без превышения допустимого уровня аккумулируемого шума.
- Прокладка оптического кабеля. Одно из решений проблемы внешних помех состоит в прокладке оптического кабеля от распределительных устройств как можно ближе к абонентам. Помимо всего прочего, это позволяет увеличить совокупную емкость кабельной сети, снизить стоимость владения и устранить необходимость использовать множество усилителей для восстановления сигнала. Однако лишь сравнительно небольшая доля кабельной инфраструктуры США (вероятно, менее 20% от всех домов, к которым она была проложена) модернизирована с помощью оптических кабелей. С технической точки зрения модернизация не представляет трудностей, но с финансовой — она оказывается весьма обременительной.
- Сокращение числа подключенных к данному сегменту кабеля. Другое потенциальное решение для уменьшения внешних помех состоит в сокращении числа подключенных к данному сегменту кабеля квартир (домов). Трудности здесь все те же — чисто экономические, потому что при прочих равных условиях кабельным операторам выгоднее иметь крупные разделяемые сегменты.

Что такое кабельный модем

Кабельным модемом называется абонентское устройство, обеспечивающее высокоскоростной доступ к Интернету по сетям кабельного телевидения, они используют асимметричную технологию, которая наи-

более оптимально подходит для пользовательского доступа к Интернету. При этом максимально возможная скорость приема данных таким модемом, может достигать порядка 40 Мбит/с и скорость передачи данных порядка 10 Мбит/с. Как и модем, предназначенный для соединения по коммутируемым телефонным линиям, это устройство представляет собой двунаправленный аналогово-цифровой преобразователь данных, использующий в процессе передачи информации принцип наложения на несущую частоту модулированного аналогового сигнала. Существенным отличием данного аппаратного средства от обыкновенного модема является то, что кабельный модем не требует установки каких-либо драйверов, поскольку он подключается к компьютеру посредством сетевой карты и является абсолютно прозрачным для системы: машина считает, что она работает в локальной сети.

Для передачи данных используется один или несколько свободных от телепередач телевизионных каналов. Передача данных и телевизионных программ ведутся одновременно, по одному и тому же кабелю, совершенно не мешая друг другу.

Применение подобных модемов ориентировано прежде всего на домашних пользователей, поскольку линии кабельного телевидения существуют в основном в жилых кварталах, тем не менее в последнее время сети кабельного телевидения начинают охватывать и административно-промышленные районы.

Устройство кабельного модема

Подключение кабельного модема осуществляется обычно через разделитель. Разделитель, в соответствии со своим названием, делит сигнал между телевизором и кабельным модемом. К одному из выходов разделителя и подключается кабельный модем. Несмотря на многочисленные отличия в конструкции, все модемы имеют одну и ту же базовую архитектуру.

К разделителю (фактически — телевизионной антенне) модем подключается через тюнер. Обычно тюнер имеет встроенный дуплексор для приема и передачи сигналов. Принятый сигнал подается на демодулятор. Данный блок выполняет функции преобразования сигнала из аналоговой в цифровую форму, демодуляции QAM-64/256, синхронизации кадров MPEG и коррекции ошибок в соответствии с кодом Рида-Соломона.

Его двойником является пакетный модулятор; он соответствующим образом модулирует сигнал для его последующей передачи на оконечную станцию и выполняет все те же операции, но в обратной последовательности. Исходящий сигнал пропускается через задающий

усилитель для обеспечения требуемой мощности сигнала. Часто и демодулятор, и модулятор реализуются в виде одной микросхемы.

Блок контроля доступа к среде передачи (Media Access Conrol, MAC) служит, с одной стороны, начальной точкой для исходящего пути, а с другой — конечной точкой для входящего пути. Ввиду сложности применяемых алгоритмов реализация функций уровня MAC требует применения микропроцессоров. Для этого используются микропроцессоры PowerPC компании Motorola или другие RISC-процессоры.

MAC протокол

Протокол MAC уровня управляет доступом к обратному каналу. Иногда данные для передачи имеются у нескольких модемов одновременно. В этих случаях MAC протокол предоставляет критерии, в соответствии с которыми системный терминал определяет последовательность доступа модемов к обратному каналу, а также время доступа для каждого модема.

Если кабельные модемы ведут передачу по очереди, никаких столкновений в обратном канале не возникает, и система работает эффективно. Столкновения вынуждают модемы посылать данные повторно, что снижает эффективность работы системы. Это, в частности, означает, что MAC протокол влияет на эффективность использования полосы обратного канала CKM.

На сегодняшний день существуют две категории CKM. Одна категория объединяет системы с индивидуальными версиями MAC протоколов. Некоторые из них предлагают сильные решения, базирующиеся в основном на ATM протоколе. Другие чаще всего базируются на стандарте IEEE 802.14 для CKM протоколов MAC уровня. Они имеют ограниченные возможности организации работы обратного канала в области избегания столкновений, обеспечения качества услуг и т.д.

После обработки в блоке MAC данные передаются на компьютер через интерфейс. Помимо Ethernet на 10 Мбит/с это может быть также USB, PCI.

Как работают кабельные модемы

В настоящее время в мире существует 2 класса оборудования для передачи данных через сети кабельного телевидения. Эти классы сформировались исторически и отличаются способом организации приема данных от абонента.

Первые попытки использовать сети кабельного телевидения для доступа к Интернету были предприняты довольно давно. Сети кабельного телевидения в то время строились на основе коаксиального кабеля по

технологии которая обеспечивала только однонаправленную передачу информации (ведь задачи организации обратной связи от абонента в сети CATV в то время не ставилось).

Поэтому первые кабельные модемы использовали технологию, при которой абонент получал данные по высокоскоростному каналу сети CATV, а исходящий поток данных к интернет-провайдеру организовывался с использованием обычного коммутируемого соединения по телефонной линии (например, с использованием дополнительного аналогового или ISDN-модема).

Данная технология получила название TELCO-Return и широко используется в настоящее время.

К достоинствам технологии TELCO-Return можно отнести:

- отсутствие необходимости изменять существующую кабельную инфраструктуру оператора CATV;
- минимальные начальные затраты для ISP при любой кабельной инфраструктуре оператора CATV.

К недостаткам можно отнести:

- наличие соединения по коммутируемой линии, что снижает общую надежность, т.к. проблемы с передачей данных по телефонной линии отразятся и на высокоскоростном приеме данных;
- затруднительно организовать постоянное подключение (24 часа в сутки) по коммутируемой линии;
- низкоскоростной поток данных от пользователей (до 33,6 Кбит/с при использовании аналогового модема на обратном канале).

В настоящее время наибольшее распространение получают гибридные сети, состоящие из участков оптического и коаксиального кабеля (так называемые «сети HFC»).

В таких сетях, при использовании двунаправленных промежуточных усилителей достигается возможность не только передавать поток данных к абоненту, но и получать обратный поток (данные от абонента). При этом можно сказать, что абонент получает возможность интерактивной работы.

Это открывает новые возможности для организации передачи данных и доступа к Интернету, позволяет использовать кабель системы кабельного телевидения уже для двунаправленной передачи данных

пользователя. При этом как высокоскоростной входящий поток, так и более медленный исходящий поток передаются по одному и тому же коаксиальному кабелю.

Данная технология получила название Cable-Return. К достоинствам технологии Cable-Return можно отнести:

- отсутствие трафика через коммутируемую телефонную сеть;
- высокоскоростной поток данных от пользователя (до 10 Мбит/с);
- высоконадежная связь с возможностью организации доступа в течение 24 часов в сутки.

К недостаткам можно отнести:

- необходимость изменять традиционную однонаправленную кабельную инфраструктуру и обеспечивать переход к двунаправленной технологии;
- ограничено количество подключенных в каждом сегменте пользователей из-за дополнительных шумов, вносимых в кабель при каждом дополнительном подключении и ограниченности диапазона частот выделенного для организации обратных каналов.

Обе эти технологии позволяют пользователю получать высокоскоростной поток данных со скоростью порядка 40 Мбит/с. Но реальная скорость принимаемых данных обычно не превышает 10 Мбит/с, в связи с ограничением, накладываемым максимальной скоростью для интерфейса Ethernet 10BASE-T, и количеством пользователей, одновременно работающих на данном канале (чем больше пользователей в сегменте одновременно использует этот частотный канал, тем меньше итоговая скорость поступления данных к каждому конкретному пользователю). Например, при 5 пользователях, одновременно принимающих файлы, скорость поступления данных к каждому отдельному пользователю будет порядка 40/5=8 Мбит/с (что в любом случае значительно превышает скорость, обеспечиваемую аналоговыми или ISDN-модемами, и делает применение кабельных модемов очень перспективным).

Архитектура кабельной сети и ее реализация в распространенных моделях кабельных модемов

Существует две архитектуры кабельной сети — симметричная и асимметричная. При использовании симметричной архитектуры для передачи данных оба сигнала — прямой и обратный — передаются по одному кабелю. Чтобы разделить прямой и обратный сигналы, их необходимо передавать в различных диапазонах частот. Учитывая это, прямая и обратная передачи происходят с разными скоростями, что, собственно, является существенным недостатком.

Симметричная архитектура имеет ряд существенных недостатков, ограничивающих ее применение:

- Устанавливать высокоскоростную связь через симметричную кабельную сеть сложно и дорого, так как обратная передача сигнала выполняется неэффективно.
- Прямая передача сигнала сильно влияет на обратную, поскольку вся информация передается по одному каналу.
- Маршрутизация и безопасность рассматриваются как внешние элементы системы.

Именно поэтому производители кабельных модемов отдают предпочтение асимметричной архитектуре, которая обладает следующими преимуществами:

- Широко используется в беспроводных сетях, поскольку обратную связь со станцией часто приходится выполнять с помощью телефона или ISDN.
- Можно создать канал с минимальной разницей скоростей прямой и обратной передачи сигнала.
- Минимальные требования к обратной передаче информации.
- Разделение прямого и обратного каналов передачи дает возможность использовать существующее оборудование для передачи данных от станции к пользователю.
- Асимметричные системы могут быть построены достаточно быстро, поскольку уже есть необходимая инфраструктура кабельного телевидения и телефонной сети.
- Гибридная архитектура с раздельными каналами для прямой и обратной передачи сигнала может обеспечить различные способы и скорости передачи информации.
- Асимметричная архитектура обеспечивает хорошую настройку системы на изменение внешних условий, оставаясь при этом надежной и недорогой.

Поэтому некоторые фирмы, выпускающие кабельные модемы, используют для своих устройств более привлекательную, асимметричную архитектуру кабельной сети. Так, например, в кабельных модемах ZENITH предлагается симметричная схема, то есть схема с одинаковой скоростью передачи данных в прямом и обратном направлении на одной из двух скоростей — 4 Мб/с или 500 Кб/с. Модем SUPERSURFR фирмы MOTOROLA обеспечивает асимметричную схему со скоростями 10 Мб/с в прямом направлении и 768 Кб/с в обратном. Кабельный модем LCP (LANCITY, BAYNETWORKS) позволяет настроить передачу как с симметричной, так и с асимметричной схемой с максимальной скоростью 10 Мб/с в обоих направлениях. MAC-подуровень управляет доступом сетевых узлов к среде передачи данных. В ZENITH реализован стандартный ETHERNET-протокол CSMA/CD, и, следовательно, приоритет доступа никак не контролируются. В CYBERSURFR используется детерминированный подход, базирующийся на опросе узлов о необходимости передать данные. LCP использует собственный протокол UNILINK, сочетающий оба подхода и основанный на выделении временных слотов для передачи данных.

Существует два подхода во взаимодействии между головным и пользовательским модемом — первый, когда и головной, и пользовательский модем принимают участие в управлении передачей данных, например, настройкой скорости, адресов, приоритетов и т.д. (PEER-TO-PEER MODEL), и второй, когда все управление сетью кабельных модемов осуществляется с головного модема (MASTER/SLAVE MODEL). Сегодня второй подход постепенно становится преобладающим, поскольку обеспечивает больший контроль за состоянием устройств, управляемость параметрами и секретность передачи данных.

Обе архитектуры — симметрична и асимметричная — могут хорошо дополнять друг друга. Например, вы можете использовать для отправки запросов подключение по коммутируемой телефонной линии, а для приема данных — кабель. Какой же архитектуре отдать предпочтение?

Передача информации по кабельным сетям может использоваться для различных целей. В промышленности, где кабельная сеть создается самим предприятием для пересылки информации, разумно использовать симметричную архитектуру, поскольку в этом случае скорость обратной и прямой передачи одинакова. Для существующих модемов она составляет примерно 10 Мб/с (LANCITY), то есть сопоставима со скоростью передачи в ETHERNET.

Для подключения домашнего компьютера к Интернету или другой глобальной сети, видимо, придется использовать асимметричную архитектуру. Существующая кабельная сеть, к которой можно подключить домашний компьютер, предназначена для телевизионных сигналов и не позволяет передавать обратный сигнал с достаточно высокой скоростью. Обычно пользователи домашнего компьютера используют связь с Интернетом для доступа к WWW и телеконференциям, а для этого требуется передача большего количества данных от станции к пользователю, а не наоборот. Чтобы получать графические, звуковые и видеофайлы из сети, требуются большие скорости передачи от станции к клиенту. Выполнение же URL-запросов или передача электронной почты не порождают большого потока данных от пользователя к станции. Поэтому передачу обратного сигнала можно выполнять с меньшей скоростью, например по телефонной линии.

Сетевой сервис сетей кабельных модемов

CKM представляют собой новый тип коммуникационной технологии для сетей городского масштаба (metropolitan area network — MAN). Очень типичной является ситуация, когда к сети подсоединяются разные категории абонентов с различными требованиями к уровню сервиса (скорости доступа, надежности и скорости передачи информации, возможностям передачи частной закрытой информации).

Набор механизмов, позволяющих удовлетворить эти требования, называется сетевыми услугами. Наиболее важными сетевыми услугами являются следующие:

- Управление качеством услуг (QoS)

Эта функция позволяет кабельному оператору задавать различные категории сервиса с гарантированными диапазоном скоростей потока и приоритетами предоставления канала. Это дает кабельному оператору возможность дифференцировать набор предоставляемых услуг (равно как и абонентскую плату) для разных категорий абонентов. Эта функция оптимизирует условия получения прибыли от эксплуатации кабельной сети. Ниже приведены основные механизмы управления качеством услуг:

1. Число уровней сервиса: Уровни сервиса позволяют назначать приоритеты доступа к каналу в зависимости от требуемых услуг.

2. Автоматическая регулировка трафика: Эта функция позволяет перераспределять ресурсы выделенных обратных каналов при их неравномерной загрузке.

3. Гарантированная скорость потока: Разные виды услуг предъявляют неодинаковые требования к постоянству скорости потока. Голос или видео требуют постоянной скорости передачи — CBR (constant bit

rate). С другой стороны, Интернет или передача данных нечувствительны к колебаниям скорости передачи. Они могут передаваться по каналам с переменной скоростью — VBR (varaible bit rate). Если в CKM реализуются разные типы услуг, то она должна поддерживать оба типа передачи — CBR и VBR:

- Поддержка виртуальной частной сети — VPN (virtual private networking)

VPN позволяет кабельным операторам реализовать защиту частной информации от несанкционированного доступа. Такое требование выдвигается высокоприбыльными абонентами с SO-HO (small office-home office), участниками телеконференций и корпоративными абонентами. Реализация этой функции в разных CKM может существенно отличаться. Различия, в первую очередь, касаются числа поддерживаемых VPN и возможной степени защищенности информации.

Система Сетевого Управления

Все сетевые услуги CKM, равно как конфигурирование CKM, а также управление и мониторинг обеспечиваются системой сетевого управления (network management system — NMS).

- дистанционное конфигурирование и мониторинг кабельных модемов

Реализация этой функции обязательно должна быть предусмотрена в NMS. Она особенно полезна при установке кабельных модемов, их реконфигурации (добавлении, сокращении или изменении сервисных услуг), дистанционной загрузке программного обеспечения и т.д.

- работа NMS

1. Ведение статистики. Для выполнения своих функций NMS вынуждена оперировать большими объемами информации. Перерабатываемая информация может представлять и самостоятельный интерес для кабельного оператора. Ввиду огромного объема этой информации, ее обработка вручную вестись не может. Более изощренные NMS обрабатывают эту информацию и выдают результаты в графической форме или в виде таблиц.

2. Механизмы контроля использования частотной полосы. Эти механизмы поставляют операторам информацию об использовании системных ресурсов. Они помогают выявить необходимость добавления ресурсов, определить типовой трафик для каждого ресурса, отследить рост востребованности сетевых ресурсов.

3. Счетные механизмы. Эти механизмы отслеживают использование кабельных модемов, что затем может использоваться при составлении счетов.

4. Механизмы планирования загрузки. Эти механизмы позволяют просчитать реакцию CKM на различные варианты использования полосы, разнообразные сочетания предоставляемых услуг, различное количество абонентов. Таким образом, механизмы планирования загрузки помогают кабельному оператору вовремя выявить необходимость подключения нового оборудования.

5. Измерение и статистика отношения сигнал/шум (CNR). Как уже отмечалось, наиболее негативным фактором, воздействующим на передачу по обратному каналу, являются шумы ингрессии. Природа возникновения этих шумов затрудняет фиксацию их появления с помощью обычного измерительного оборудования. Наиболее изощренные NMS способны постоянно сканировать полосу обратного канала, измеряя шумы ингрессии. Такие NMS обеспечивают одновременно и мониторинг обратного канала.

- протокол управления NMS и графический интерфейс пользователя

CKM может быть не единственной телекоммуникационной системой кабельной сети, в которой реализуется управление и мониторинг. В этих случаях отдельные NMS объединяются в интегрированную систему.

Для такого объединения требуется, чтобы во всех NMS использовался одинаковый управляющий протокол. Широко распространен Simple Network Management protocol (SNMP). Системы, использующие SNMP, легко объединяются в одну общую систему управления.

Для облегчения и большего удобства работы оператора в NMS предусматривается графический интерфейс пользователя. Наиболее распространенный интерфейс — H-P Open View visualization SW.

Преимущества кабельных модемов перед другими технологиями высокоскоростной передачи данных

Основным преимуществом кабельных модемов, по сравнению с аналоговыми и ISDN модемами, является высокая скорость принимаемых данных, недостижимая даже для большинства дорогостоящих xDSL модемов.

Вторым важным преимуществом кабельных модемов является низкая стоимость подключения по сравнению с арендой линии ISDN.

Чрезвычайно высокая скорость получения информации, сравнимая со скоростями в локальных сетях Ethernet, позволяет использовать кабельные модемы для работы во многих высокоскоростных приложениях реального времени (в том числе сетевых компьютерных играх).

Проблемы кабельных модемов

Перед внедрением любой новой технологии необходимо решить ряд задач, которые могут быть не только техническими, но и экономическими или организационными. Это же относится и к кабельным модемам. Здесь возникают следующие проблемы:

- **Управление сетью.** Провайдеры должны постоянно контролировать работу кабельной сети и правильно управлять ею.
- **Технические проблемы.** Фирмам-производителям кабельных модемов придется разработать надежную архитектуру, обеспечивающую совместимость кабельных сетей различных провайдеров и согласовать стандарты передачи сигналов по ним.
- **Шифрование данных.** Для кабельной сети, которая может быть подключена к любому зданию в городе, важно сохранить конфиденциальность данных. Для этого, видимо, необходимо использовать специальные устройства для шифрования сигнала или данных.
- **Удобство использования.** Кабельный модем должен иметь различные полезные свойства, например контроль скорости передачи, поддержку нескольких компьютеров или даже локальной сети, возможность определения своего места в сети и так далее.
- **Различные методы обратной передачи.** Небольшим компаниям, которые будут предлагать услуги для доступа к Интернету через кабельное телевидение, по-видимому, не удастся обеспечить в своих сетях двусторонний доступ. Их клиенты смогут получить доступ к Интернету с помощью асимметричной архитектуры сети, т. е. обратный сигнал будет передаваться по телефону.

- **Стоимость.** Цена кабельного модема должна быть сопоставима с ценой высокоскоростного телефонного модема.

Стандарты DOCSIS и EuroDOCSIS

В 1998 г. на сессии рабочей группы ITU в Женеве был одобрен основополагающий стандарт J.112, определяющий методы передачи данных по сетям кабельного телевидения. Базируясь на основе стандартов ITU J.112 и J.83, консорциумом CableLabs в сотрудничестве с широким кругом производителей оборудования был разработан единый международный стандарт, известный под названием Data Over Cable Service Interface Specification (DOCSIS).

Этот стандарт предусматривает передачу данных абоненту по сети кабельного телевидения с максимальной скоростью до 42 Мбит/с (при ширине полосы пропускания 6 МГц и использовании многопозиционной амплитудной модуляции 256 QAM) и получение данных от абонента со скоростью до 10,24 Мбит/с. Он призван сменить господствовавшие ранее решения на основе фирменных протоколов передачи данных и методов модуляции, несовместимых друг с другом, и должен гарантировать совместимость аппаратуры различных производителей.

Принятые ITU документы содержат также три приложения, учитывающие специфические особенности американского, европейского и японского рынков услуг CATV и используемые в этих регионах стандарты (NTSC, PAL, SECAM).

EuroDOCSIS регламентирует принятое для Европы распределение частот прямого и обратного канала, оговаривает работу с полосой 8 МГц.

Стандарт DOCSIS 1.1 дополнительно предусматривает наличие специальных механизмов, улучшающих поддержку IP-телефонии, уменьшающих задержки при передаче речи (например, механизмы фрагментации и сборки больших пакетов, организации виртуальных каналов и задания приоритетов).

DOCSIS имеет прямую поддержку IP протокола, с нефиксированной длиной пакетов. DVR-RC, в свою очередь, для передачи IP пакетов использует ATM Cell transport, то есть, IP пакет сначала переводится в формат ATM, который и передается по кабелю. На другой, стороне, производится обратный процесс. Фиксированный размер ATM пакетов, не позволяет работать таким службам, как Voice over IP (передача голосовой и видеоинформации), недостаток, которого лишен DOCSIS. К тому же, большинство IP пакетов немного больше ATM пакетов, поэтому для пе-

редачи одного IP пакета приходится использовать два ATM пакета, что приводит к потерям в 30–50%, чем и обусловлена меньшая эффективность и производительность этого стандарта.

Поддержка трехслойного мультипротокола:

- Разные абоненты используют в своих LAN и PC различные трехслойные протоколы. Технология CKM обеспечивает мультипротокольную работу, позволяющую подключать абонентов к сети вне зависимости от протоколов, которые используют их приложения. Это обстоятельство существенно облегчает включение абонентских приложений в кабельную сеть. Наиболее распространены трехуровневые протоколы TCP/IP, SPX/IPX, AppleTalk и NetBEUI.
- Если CKM поддерживает только TCP/IP, то кабельный оператор не сможет подсоединить абонентов, работающих в других протоколах. Например, не смогут быть подсоединены сети Novell 3 или Novell 4. Если CKM не поддерживает NetBEUI, то абонент не сможет использовать сетевые механизмы Microsoft.

Защита данных

Совместная работа нескольких пользователей по общему кабелю имеет определенные особенности, требующие принятия специальных мер для обеспечения защиты информации.

В разделяемой сети каждый узел имеет возможность, по крайней мере, на физическом уровне, видеть трафик ко всем остальным узлам. Точно так же, как весь трафик в сегменте Ethernet виден протокольному анализатору при использовании сетевой платы с поддержкой режима приема всех пакетов, протокольный анализатор может перехватывать весь трафик в сегменте сети КТВ, если не будут приняты меры защиты. Как показывает практика, по крайней мере, в одном зарегистрированном случае пользователь кабельного модема с сетевым клиентом Windows мог видеть свыше 100 разделяемых дисков в настольных системах своих соседей.

Обеспечению конфиденциальности и защите данных в сетях кабельного телевидения уделяется серьезное внимание. Фактический стандарт в лице спецификации интерфейса для служб передачи данных по кабельной сети (Data-over-Cable Service Interface Specification, DOCSIS) был предложен отраслевой группой Multimedia Cable Network System (MCNS). Он предусматривает установку средств шифрования

DES на каждый модем. При этом данные каждого пользователя передаются по кабелю только в зашифрованном виде с использованием индивидуального ключа шифрования. Это решение, или любая форма шифрования вообще, является, по-видимому, необходимым для защищенной передачи информации по сетям кабельного телевидения. Однако применение дополнительного оборудования увеличивает общую стоимость модемов и административную нагрузку и к тому же повышает требования к техническому персоналу кабельного оператора.

Большинство кабельных модемов имеют встроенные мосты уровня MAC, лишающие абонентов возможности видеть любые кадры, помимо предназначенных непосредственно им. Мосты, однако, не блокируют широковещательные кадры, поэтому беспринципные пользователи имеют возможность осуществлять атаки типа «отказ в обслуживании» на своих соседей.

Еще одно возможное решение предусматривает установку брандмауэра позади кабельного модема, но, опять же, финансовые и административные расходы оказываются весьма высокими.

Данные меры препятствуют перехвату трафика в сегменте сети и обеспечивают надежную защиту передаваемой информации.

Применение кабельных модемов

Использование кабельных модемов не ограничивается только получением огромного количества нужной и ненужной информации через Интернет в окна браузера и, как следствие, на жесткий диск вашего компьютера. Используя кабельную сеть, можно построить очень даже неплохую интрасеть в вашем доме. Да и офисы компаний можно оснастить интрасетями, основанными на данной технологии, — чем не альтернатива выделенным линиям? Прибавьте сюда отличную возможность организации видеоконференций (в элитных домах это может быть видеотелефон) и много-много всякой всячины, которая так разнообразит ваш досуг с компьютером.

Возвращаясь к серьезности технологий, можно найти еще много различных сфер применения кабельных технологий. Например, в области образования и автоматизации процесса обучения. Представьте школу, оснащенную, во-первых, компьютерами, во-вторых, кабельной сетью. Думаю, нашей системе образования надо подумать об этом, ведь данные технологии значительно расширяют возможности устаревших лингафонных классов или скучных уроков информатики. Познакомить подрастающее поколение с современными технологиями значит, заложить камень в собственное будущее. Уверен, что школьники, получившие в свое распоряжение такую локальную и глобальную сеть, с огромным удоволь-

ствием будут до позднего вечера коротать время в школе, находя ей применение. Еще одна отрасль — медицина: наблюдение за пациентами, видеодиагностика и так далее.

Увеличение скорости обмена информацией, которое обещает технология кабельных модемов, может повлиять почти на все области человеческой деятельности. Кабельное телевидение всегда было предназначено для развлечений, поэтому логично использовать его и для распределенных компьютерных игр. Но кабельный модем позволяет использовать развлекательные системы для работы и для делового общения, для обучения и лечения. Границы этой новой технологии еще трудно определить, но уже ясно одно: кабельный модем впустит Интернет в каждый дом.

Технологии xDSL. Стандарт G.992.2 (G.Lite)

Увеличение потоков информации, передаваемых по сети Интернет компаниями и частными пользователями, а также потребность в организации удаленного доступа к корпоративным сетям, породили потребность в создании недорогих технологий цифровой высокоскоростной передачи данных по самому «узкому» месту цифровой сети — абонентской телефонной линии. Технологии DSL позволяют значительно увеличить скорость передачи данных по медным парам телефонных проводов без необходимости модернизации абонентских телефонных линий. Именно возможность преобразования существующих телефонных линий в высокоскоростные каналы передачи данных и является главным преимуществом технологий DSL. Считается, что стандарт G.Lite, описывающий одну из разновидностей технологии цифровых абонентских линий, позволит продвинуть широкополосный доступ к Интернету на потребительский рынок.

Технологии DSL

Современный мир созрел для использования технологий DSL. Увеличение потоков информации, передаваемых по сети Интернет компаниями и частными пользователями, а также потребность в организации удаленного доступа к корпоративным сетям, породили потребность в создании недорогих технологий цифровой высокоскоростной передачи данных по самому «узкому» месту цифровой сети — абонентской телефонной линии.

Технологии DSL позволяют значительно увеличить скорость передачи данных по медным парам телефонных проводов без необходимости модернизации абонентских телефонных линий. Именно возможность преобразования существующих телефонных линий в высокоскоростные каналы передачи данных и является главным преимуществом технологий DSL.

Сокращение DSL расшифровывается как Digital Subscriber Line (цифровая абонентская линия). DSL является достаточно новой технологией, позволяющей значительно расширить полосу пропускания старых медных телефонных линий, соединяющих телефонные станции с индивидуальными абонентами. Любой абонент, пользующийся в настоящий момент обычной телефонной связью, имеет возможность с помощью технологии DSL значительно увеличить скорость своего соединения, например, с сетью Интернет. Следует помнить, что для организации линии DSL используются именно существующие телефонные линии; данная технология тем и хороша, что не требует прокладывания дополнительных телефонных кабелей. В результате вы получаете круглосуточный доступ в сеть Интернет с сохранением нормальной работы обычной телефонной связи. Никто из ваших друзей больше не пожалуется, что часами не может к вам прозвониться.

Благодаря многообразию технологий DSL пользователь может выбрать подходящую именно ему скорость передачи данных — от 32 Кбит/с до более чем 50 Мбит/с. Данные технологии позволяют также использовать обычную телефонную линию для таких широкополосных систем, как видео по запросу или дистанционное обучение. Современные технологии DSL приносят возможность организации высокоскоростного доступа в Интернет в каждый дом или на каждое предприятие среднего и малого бизнеса, превращая обычные телефонные кабели в высокоскоростные цифровые каналы. Причем скорость передачи данных зависит только от качества и протяженности линии, соединяющих пользователя и провайдера. При этом провайдеры обычно дают возможность пользователю самому выбрать скорость передачи, наиболее соответствующую его индивидуальным потребностям.

Как работает DSL

Телефонный аппарат, установленный у вас дома или в офисе, соединяется с оборудованием телефонной станции с помощью витой пары медных проводов. Традиционная телефонная связь предназначена для обычных телефонных разговоров с другими абонентами телефонной сети. При этом по сети передаются аналоговые сигналы. Телефонный аппарат воспринимает акустические колебания (являющиеся естественным аналоговым сигналом) и преобразует их в электрический сигнал, амплитуда и частота которого постоянно изменяется. Так как вся работа телефонной сети построена на передаче аналоговых сигналов, проще всего, конечно же, использовать для передачи информации между або-

нентами или абонентом и провайдером именно такой метод. Именно поэтому вам пришлось прикупить в дополнение к вашему компьютеру еще и модем, который позволяет демодулировать аналоговый сигнал и превратить его в последовательность нулей и единиц цифровой информации, воспринимаемой компьютером.

При передаче аналоговых сигналов используется только небольшая часть полосы пропускания витой пары медных телефонных проводов; при этом максимальная скорость передачи, которая может быть достигнута с помощью обычного модема, составляет около 56 Кбит/с. DSL представляет собой технологию, которая исключает необходимость преобразования сигнала из аналоговой формы в цифровую форму и наоборот. Цифровые данные передаются на ваш компьютер именно как цифровые данные, что позволяет использовать гораздо более широкую полосу частот телефонной линии. При этом существует возможность одновременно использовать и аналоговую телефонную связь, и цифровую высокоскоростную передачу данных по одной и той же линии, разделяя спектры этих сигналов.

Различные типы технологий DSL и краткое описание их работы

DSL представляет собой набор различных технологий, позволяющих организовать цифровую абонентскую линию. Для того, чтобы понять данные технологии и определить области их практического применения, следует понять, чем эти технологии различаются. Прежде всего, всегда следует держать в уме соотношение между расстоянием, на которое передается сигнал, и скоростью передачи данных, а также разницу в скоростях передачи «нисходящего» (от сети к пользователю) и «восходящего» (от пользователя в сеть) потока данных.

DSL объединяет под своей крышей следующие технологии.

- ADSL (Asymmetric Digital Subscriber Line — асимметричная цифровая абонентская линия)

Данная технология является асимметричной, то есть скорость передачи данных от сети к пользователю значительно выше, чем скорость передачи данных от пользователя в сеть. Такая асимметрия, в сочетании с состоянием «постоянно установленного соединения» (когда исключается необходимость каждый раз набирать телефонный номер и ждать установки соединения), делает технологию ADSL идеальной для организации доступа в сеть Интернет, доступа к локальным сетям (ЛВС) и т.п. При организации таких соединений пользователи обычно получают гораздо больший объем информации, чем передают. Технология ADSL

обеспечивает скорость «нисходящего» потока данных в пределах от 1,5 Мбит/с до 8 Мбит/с и скорость «восходящего» потока данных от 640 Кбит/с до 1,5 Мбит/с. ADSL позволяет передавать данные со скоростью 1,54 Мбит/с на расстояние до 5,5 км по одной витой паре проводов. Скорость передачи порядка 6 — 8 Мбит/с может быть достигнута при передаче данных на расстояние не более 3,5 км по проводам диаметром 0,5 мм.

- R-ADSL (Rate-Adaptive Digital Subscriber Line — цифровая абонентская линия с адаптацией скорости соединения)

Технология R-ADSL обеспечивает такую же скорость передачи данных, что и технология ADSL, но при этом позволяет адаптировать скорость передачи к протяженности и состоянию используемой витой пары проводов. При использовании технологии R-ADSL соединение на разных телефонных линиях будет иметь разную скорость передачи данных. Скорость передачи данных может выбираться при синхронизации линии, во время соединения или по сигналу, поступающему от станции.

- ADSL Lite

ADSL Lite представляет собой низкоскоростной (относительно, конечно же) вариант технологии ADSL, обеспечивающий скорость «нисходящего» потока данных до 1 Мбит/с и скорость «восходящего» потока данных до 512 Кбит/с. Технология ADSL Lite позволяет передавать данные по более длинным линиям, чем ADSL, более проста в установке и имеет меньшую стоимость, что обеспечивает ее привлекательность для массового пользователя.

- IDSL (ISDN Digital Subscriber Line — цифровая абонентская линия IDSN)

Технология IDSL обеспечивает полностью дуплексную передачу данных на скорости до 144 Кбит/с. В отличие от ADSL возможности IDSL ограничиваются только передачей данных. Несмотря на то, что IDSL также как и ISDN использует модуляцию 2B1Q, между ними имеется ряд отличий. В отличие от ISDN линия IDSL является некоммутируемой линией, не приводящей к увеличению нагрузки на коммутационное оборудование провайдера. Также линия IDSL является «постоянно включенной» (как и любая линия, организованная с использованием технологии DSL), в то время как ISDN требует установки соединения.

- HDSL (High Bit-Rate Digital Subscriber Line — высокоскоростная цифровая абонентская линия)

Технология HDSL предусматривает организацию симметричной линии передачи данных, то есть скорости передачи данных от пользова-

теля в сеть и из сети к пользователю равны. Благодаря скорости передачи (1,544 Мбит/с по двум парам проводов и 2,048 Мбит/с по трем парам проводов) телекоммуникационные компании используют технологию HDSL в качестве альтернативы линиям T1/E1. (Линии T1 используются в Северной Америке и обеспечивают скорость передачи данных 1,544 Мбит/с, а линии E1 используются в Европе и обеспечивают скорость передачи данных 2,048 Мбит/с.) Хотя расстояние, на которое система HDSL передает данные (а это порядка 3,5–4,5 км), меньше, чем при использовании технологии ADSL, для недорогого, но эффективного, увеличения длины линии HDSL телефонные компании могут установить специальные повторители. Использование для организации линии HDSL двух или трех витых пар телефонных проводов делает эту систему идеальным решением для соединения УАТС, серверов Интернет, локальных сетей и т.п. Технология HDSL II является логическим результатом развития технологии HDSL. Данная технология обеспечивает характеристики, аналогичные технологии HDSL, но при этом использует только одну пару проводов.

- SDSL (Single Line Digital Subscriber Line — однолинейная цифровая абонентская линия)

Также как и технология HDSL, технология SDSL обеспечивает симметричную передачу данных со скоростями, соответствующими скоростям линии T1/E1, но при этом технология SDSL имеет два важных отличия. Во-первых, используется только одна витая пара проводов, а во-вторых, максимальное расстояние передачи ограничено 3 км. В пределах этого расстояния технология SDSL обеспечивает, например, работу системы организации видеоконференций, когда требуется поддерживать одинаковые потоки передачи данных в оба направления. В определенном смысле технология SDSL является предшественником технологии HDSL II.

- VDSL (Very High Bit-Rate Digital Subscriber Line — сверхвысокоскоростная цифровая абонентская линия)

Технология VDSL является наиболее «быстрой» технологией xDSL. Она обеспечивает скорость передачи данных «нисходящего» потока в пределах от 13 до 52 Мбит/с, а скорость передачи данных «восходящего» потока в пределах от 1,5 до 2,3 Мбит/с, причем по одной витой паре телефонных проводов. Технология VDSL может рассматриваться как экономически эффективная альтернатива прокладыванию волоконно-оптического кабеля до конечного пользователя. Однако, максимальное расстояние передачи данных для этой технологии составляет от 300 метров до 1300 метров. То есть, либо длина абонентской линии не должна превышать данного значения, либо оптико-волоконный кабель должен

быть подведен поближе к пользователю (например, заведен в здание, в котором находится много потенциальных пользователей). Технология VDSL может использоваться с теми же целями, что и ADSL; кроме того, она может использоваться для передачи сигналов телевидения высокой четкости (HDTV), видео по запросу и т.п.

Технологии DSL, позволяющие передавать голос, данные и видеосигнал по существующей кабельной сети, состоящей из витых пар телефонных проводов, наилучшим образом отражают потребность пользователей в высокоскоростных системах передачи.

Во-первых, технологии DSL обеспечивают высокую скорость передачи данных. Различные варианты технологий DSL обеспечивают различную скорость передачи данных, но в любом случае эта скорость гораздо выше скорости самого быстрого аналогового модема.

Во-вторых, технологии DSL оставляют вам возможность пользоваться обычной телефонной связью, несмотря на то, что используют для своей работы абонентскую телефонную линию. Используя технологии DSL вам больше не надо беспокоиться о том, что вы не получите вовремя важное известие, или о том, что для обычного телефонного звонка вам прежде потребуется выйти из сети Интернет.

И, наконец, линия DSL всегда работает. Соединение всегда установлено, и вам больше не надо набирать телефонный номер и ждать установки соединения, каждый раз, когда вы хотите подключиться. Не придется больше беспокоиться о том, что в сети произойдет случайное разъединение, и вы потеряете связь именно в тот момент, когда загружаете из сети данные, которые вам просто жизненно необходимы. Электронную почту вы будет получать в момент поступления, а не тогда, когда решите ее проверить. В общем, линия будет работать всегда, а вы будете всегда на линии.

Общее описание технологии ADSL

ADSL (Asymmetric Digital Subscriber Line — Асимметричная цифровая абонентская линия) входит в число технологий высокоскоростной передачи данных, известных как технологии DSL (Digital Subscriber Line — Цифровая абонентская линия) и имеющих общее обозначение xDSL. К другим технологиям DSL относятся HDSL (High data rate Digital Subscriber Line — Высокоскоростная цифровая абонентская линия), VDSL (Very high data rate Digital Subscriber Line — Сверхвысокоскоростная цифровая абонентская линия) и другие.

Общее название технологий DSL возникло в 1989 году, когда впервые появилась идея использовать аналого-цифровое преобразова-

ние на абонентском конце линии, что позволило бы усовершенствовать технологию передачи данных по витой паре медных телефонных проводов. Технология ADSL была разработана для обеспечения высокоскоростного (можно даже сказать мегабитного) доступа к интерактивным видеослужбам (видео по запросу, видеоигры и т.п.) и не менее быстрой передачи данных (доступ в Интернет, удаленный доступ к ЛВС и другим сетям).

Так что же такое ADSL? Прежде всего, ADSL является технологией, позволяющей превратить витую пару телефонных проводов в тракт высокоскоростной передачи данных. Линия ADSL соединяет два модема ADSL, которые подключены к каждому концу витой пары телефонного кабеля. При этом организуются три информационных канала — «нисходящий» поток передачи данных, «восходящий» поток передачи данных и канал обычной телефонной связи (POTS). Канал телефонной связи выделяется с помощью фильтров, что гарантирует работу вашего телефона даже при аварии соединения ADSL.

ADSL является асимметричной технологией — скорость «нисходящего» потока данных (т.е. тех данных, которые передаются в сторону конечного пользователя) выше, чем скорость «восходящего» потока данных (в свою очередь передаваемого от пользователя в сторону сети). Сразу же следует сказать, что не следует искать здесь причину для беспокойства. Скорость передачи данных от пользователя (более «медленное» направление передачи данных) все равно значительно выше, чем при использовании аналогового модема. Фактически же она также значительно выше, чем ISDN (Integrated Services Digital Network — Интегральная цифровая сеть связи).

Для сжатия большого объема информации, передаваемой по витой паре телефонных проводов, в технологии ADSL используется цифровая обработка сигнала и специально созданные алгоритмы, усовершенствованные аналоговые фильтры и аналого-цифровые преобразователи. Телефонные линии большой протяженности могут ослабить передаваемый высокочастотный сигнал (например, на частоте 1 МГц, что является обычной скоростью передачи для ADSL) на величину до 90 дБ. Это заставляет аналоговые системы модема ADSL работать с достаточно большой нагрузкой, позволяющей иметь большой динамический диапазон и низкий уровень шумов. На первый взгляд система ADSL достаточно проста — создаются каналы высокоскоростной передачи данных по обычному телефонному кабелю. Но, если детально разобраться в работе ADSL, можно понять, что данная система относится к достижениям современной технологии.

Технология ADSL использует метод разделения полосы пропускания медной телефонной линии на несколько частотных полос (также называемых несущими). Это позволяет одновременно передавать несколько сигналов по одной линии. Точно такой же принцип лежит в основе кабельного телевидения, когда каждый пользователь имеет специальный преобразователь, декодирующий сигнал и позволяющий видеть на экране телевизора футбольный матч или увлекательный фильм. При использовании ADSL разные несущие одновременно переносят различные части передаваемых данных.

Этот процесс известен как частотное уплотнение линии связи (Frequency Division Multiplexing — FDM). При FDM один диапазон выделяется для передачи «восходящего» потока данных, а другой диапазон для «нисходящего» потока данных. Диапазон «нисходящего» потока в свою очередь делится на один или несколько высокоскоростных каналов и один или несколько низкоскоростных каналов передачи данных. Диапазон «восходящего» потока также делится на один или несколько низкоскоростных каналов передачи данных. Кроме этого может применяться технология эхокомпенсации (Echo Cancellation), при использовании которой диапазоны «восходящего» и «нисходящего» потоков перекрываются и разделяются средствами местной эхокомпенсации.

Именно таким образом ADSL может обеспечить, например, одновременную высокоскоростную передачу данных, передачу видеосигнала и передачу факса. И все это без прерывания обычной телефонной связи, для которой используется та же телефонная линия. Технология предусматривает резервирования определенной полосы частот для обычной телефонной связи (или POTS — Plain Old Telephone Service). Удивительно, как быстро телефонная связь превратилась не только в «простую» (Plain), но и в «старую» (Old); получилось что-то вроде «старой доброй телефонной связи». Однако, следует отдать должное разработчикам новых технологий, которые все же оставили телефонным абонентам узенькую полоску частот для живого общения. При этом телефонный разговор можно вести одновременно с высокоскоростной передачей данных, а не выбирать одно из двух. Более того, даже если у вас отключат электричество, обычная «старая добрая» телефонная связь будет работать по-прежнему и с вызовом электрика у вас никаких проблем не возникнет. Обеспечение такой возможности было одним из разделов оригинального плана разработки ADSL. Даже одна эта возможность дает системе ADSL значительное преимущество перед ISDN.

Одним из основных преимуществ ADSL над другими технологиями высокоскоростной передачи данных является использование самых обычных витых пар медных проводов телефонных кабелей. Совершенно очевидно, что таких пар проводов насчитывается гораздо больше (и это

еще слабо сказано), чем, например, кабелей, проложенных специально для кабельных модемов. ADSL образует, если можно так сказать, «наложенную сеть». При этом дорогостоящей и отнимающей много времени модернизации коммутационного оборудования (как это необходимо для ISDN) не требуется.

ADSL является технологией высокоскоростной передачи данных, но насколько высокоскоростной? Учитывая, что буква «A» в названии ADSL означает «asymmetric» (асимметричная), можно сделать вывод, что передача данных в одну сторону осуществляется быстрее, чем в другую. Поэтому следует рассматривать две скорости передачи данных: «нисходящий» поток (передача данных от сети к вашему компьютеру) и «восходящий» поток (передача данных от вашего компьютера в сеть).

Факторами, влияющими на скорость передачи данных, являются состояние абонентской линии (т.е. диаметр проводов, наличие кабельных отводов и т.п.) и ее протяженность. Затухание сигнала в линии увеличивается при увеличении длины линии и возрастании частоты сигнала, и уменьшается с увеличением диаметра провода. Фактически функциональным пределом для ADSL является абонентская линия длиной 3,5–5,5 км при толщине проводов 0,5 мм. В настоящее время ADSL обеспечивает скорость «нисходящего» потока данных в пределах от 1,5 Мбит/с до 8 Мбит/с и скорость «восходящего» потока данных от 640 Кбит/с до 1 Мбит/с. Общая тенденция развития данной технологии обещает в будущем увеличение скорости передачи данных, особенно в «нисходящем» направлении.

Для того, чтобы оценить скорость передачи данных, обеспечиваемую технологией ADSL, необходимо сравнить ее с той скоростью, которая может быть доступна пользователям, использующим другие технологии. Аналоговые модемы позволяют передавать данные со скоростью от 14,4 до 56 Кбит/с. ISDN обеспечивает скорость передачи данных 64 Кбит/с на канал (обычно пользователь имеет доступ к двум каналам, что в сумме составляет 128 Кбит/с). Различные технологии DSL дают пользователю возможность передавать данные со скоростью 128 Кбит/с (IDSL), 768 Кбит/с (HDSL), «нисходящий» поток 1,5–8 Мбит/с и «восходящий» поток 640–1000 Кбит/с (ADSL), «нисходящий» поток 13–52 Мбит/с и «восходящий» поток 1,5–2,3 Мбит/с (VDSL).

Кабельные модемы имеют скорость передачи данных от 500 Кбит/с до 10 Мбит/с. (При этом следует учитывать, что полоса пропускания кабельных модемов делится между всеми пользователями, одновременно имеющими доступ к данной линии. Поэтому число одновременно работающих пользователей оказывает значительное влияние на реальную скорость передачи данных каждого из них.) Цифровые линии E1 и E3 имеют скорость передачи данных, соответственно, 2,048 Мбит/с и 34 Мбит/с.

При использовании технологии ADSL полоса пропускания той линии, с помощью которой конечный пользователь связан с магистральной сетью, принадлежит этому пользователю всегда и целиком. Нужна ли вам линия ADSL? Решать вам, но для того, чтобы вы приняли правильное решение, рассмотрим некоторые преимущества ADSL.

Прежде всего, скорость передачи данных. Цифры были указаны двумя абзацами выше. Причем эти цифры не являются пределом. В последующие годы можно ожидать увеличения скорости «нисходящего» потока до 52 Мбит/с, а «восходящего» потока до 2 Мбит/с.

Больше не нужно набирать телефонный номер для того, чтобы подключиться к сети Интернет или к ЛВС. ADSL создает широкополосный канал передачи данных, используя уже существующую телефонную линию. После установки модемов ADSL вы получаете постоянно установленное соединение. Высокоскоростной канал передачи данных всегда готов к работе — в любой момент, когда вам это потребуется.

Полоса пропускания линии принадлежит пользователю целиком. В отличие от кабельных модемов, которые допускают разделение полосы пропускания между всеми пользователями (что в значительной мере оказывает влияние на скорость передачи данных), технология ADSL предусматривает использование линии только одним пользователем.

Технология ADSL позволяет полностью использовать ресурсы линии. При обычной телефонной связи используется около одной сотой пропускной способности телефонной линии. Технология ADSL устраняет этот «недостаток» и использует оставшиеся 99% для высокоскоростной передачи данных. При этом для различных функций используются различные полосы частот. Для телефонной (голосовой) связи используется область самых низких частот всей полосы пропускания линии (приблизительно до 4 кГц), а вся остальная полоса используется для высокоскоростной передачи данных.

Многофункциональность данной системы является не самым последним аргументом в ее пользу. Так как для работы различных функций выделены различные частотные каналы полосы пропускания абонентской линии, ADSL позволяет одновременно передавать данные и говорить по телефону. Вы можете звонить по телефону и отвечать на звонки, передавать и принимать факсы, одновременно с этим находясь в сети Интернет или получая данные из корпоративной сети ЛВС. Все это по одной и той же телефонной линии.

ADSL открывает совершенно новые возможности в тех областях, в которых в режиме реального времени необходимо передавать качественный видеосигнал. К ним относится, например, организация видеоконференций, обучение на расстоянии и видео по запросу. Технология ADSL позволяет провайдерам предоставлять своим пользователям услуги, скорость передачи данных которых более чем в 100 раз превышает скорость самого быстрого на данный момент аналогового модема (56 Кбит/с) и более чем в 70 раз превышает скорость передачи данных в ISDN (128 Кбит/с).

Технология ADSL позволяет телекоммуникационным компаниям предоставлять частный защищенный канал для обеспечения обмена информацией между пользователем и провайдером.

Не следует забывать и о затратах. Технология ADSL эффективна с экономической точки зрения хотя бы потому, что не требует прокладки специальных кабелей, а использует уже существующие двухпроводные медные телефонные линии. То есть, если у вас дома или в офисе есть подключенный телефонный аппарат, вам не нужно прокладывать дополнительные провода для использования ADSL. (Хотя есть и ложка дегтя. Компания, обеспечивающая вам возможность обычной телефонной связи, должна при этом предоставлять и услугу ADSL.)

Для того, чтобы линия ADSL работала, необходимо не так уж много оборудования. На обоих концах линии устанавливаются модемы ADSL: один на стороне пользователя (дома или в офисе), а другой на стороне сети (у провайдера Интернет или на телефонной станции). Причем пользователю совсем не обязательно покупать свой модем, но достаточно взять его у провайдера в аренду. Кроме того, пользователю для того, чтобы модем ADSL работал, необходимо иметь компьютер и интерфейсную плату, например, Ethernet 10baseT.

По мере того, как телефонные компании постепенно вступают на еще неосвоенное поле передачи данных форматов видео и мультимедиа конечному пользователю, технология ADSL продолжает играть большую роль. Разумеется, через какое-то время широкополосная кабельная сеть охватит всех потенциальных пользователей. Но успех этих новых систем будет зависеть от того, какое количество пользователей будет вовлечено в процесс использования новых технологий уже сейчас. Принося кинофильмы и телевидение, видеокаталоги и Интернет в дома и офисы, ADSL делает данный рынок жизнеспособным и прибыльным как для телефонных компаний, так и для других компаний, предоставляющих услуги в различных областях.

G.Lite-доступ к Интернет для небольших офисов

Пользователи, работающие дома и в небольших офисах, с каждым днем все острее ощущают необходимость в высокоскоростном доступе к Интернет. Им уже не хватает пропускной способности 56-Кбит/с аналоговых модемов — нужны гораздо более мощные средства. С этой целью создано оборудование, работающее на базе технологий кабельных модемов, цифровой спутниковой связи, ISDN и xDSL. Из перечисленных наивысший уровень информационной безопасности обеспечивают технологии xDSL, они же гарантируют необходимую высокую скорость передачи данных. Но широкое применение таких технологий сдерживается высокой стоимостью соответствующего оборудования для поставщиков услуг, отсутствием основанных на стандартах совместимых аппаратных средств и нередко возникающими трудностями в переговорах поставщиков с местными телефонными операторами об использовании существующих абонентских линий и размещении оборудования xDSL на их узлах связи. Учитывая эти обстоятельства, МСЭ-Т принял стандарт G.Lite; предполагается, что он должен стать единым стандартом на передачу данных по технологиям xDSL и тем самым ускорить развитие рынка соответствующих услуг.

Большинство сегодняшних технологий xDSL фирменные. Каждый производитель в своих продуктах реализует свой собственный метод передачи данных, соответствующий стандарту ANSI T1.413 Issue 2, в котором указаны рекомендуемые шумовые и частотные характеристики оборудования, но не определен метод кодирования данных. Когда вы подписываетесь на услуги xDSL, вы получаете маршрутизатор или модем xDSL, совместимый с оборудованием поставщика услуг. G.Lite предназначен для стандартизации параметров передачи, что позволит пользователям свободно выбирать на рынке средства xDSL и осуществлять доступ к внешним сетям, подключая эти средства к розеткам в отелях и аэропортах.

Технология ADSL обеспечивает скорость передачи данных до 8 Мбит/с в сторону абонента и до 1,5 Мбит/с от него. Можно предположить, что благодаря асимметричности ADSL (скорости приема и передачи данных разные) предоставление местными операторами услуг ADSL не должно повредить их бизнесу по предоставлению более дорогих услуг связи на базе каналов T1. Однако многие операторы все же опасаются этого и не спешат с внедрением услуг ADSL.

Длина абонентских линий xDSL и G.Lite не превышает 5,5 км. 70–80% домов в США удалены от местных телефонных станций не более чем на 3 км, что создает хорошую предпосылку для внедрения услуг xDSL и G.Lite. Однако стоит принять во внимание тот факт, что на мед-

ных линиях связи некоторых операторов установлены пупиновские катушки (load coils), которые отфильтровывают высокочастотные шумы и улучшают качество аналоговых речевых сигналов, занимающих полосу частот ниже 4 кГц. Средства xDSL обычно передают данные по тем же самым медным линиям, но на гораздо более высоких частотах. Пупиновские же катушки благополучно отфильтровывают и их сигналы. А поставщикам услуг для обеспечения связи по технологии xDSL отнюдь не всегда удается уговорить местные операторские компании удалить эти катушки. Таким образом, следует иметь запасной вариант организации высокоскоростного доступа для пользователей, которым нельзя предоставить услуги xDSL.

В отличие от полноскоростного стандарта ADSL со скоростью передачи данных в сторону абонента до 8 Мбит/с в стандарте G.Lite этот показатель не превышает 1,5 Мбит/с, а скорость передачи данных от абонента составляет примерно 768 Кбит/с. Такое ограничение позволяет поставщикам услуг гарантировать дальность связи до 5,5 км. При длине абонентской линии свыше указанной в ней возникает больше электрических помех, снижающих скорость передачи данных. Существенно ограничив максимальную скорость, разработчики стандарта G.Lite упростили реализацию данной технологии и сделали ее более доступной для пользователей.

Технология, способная вывести DSL в массы

Считается, что стандарт G.Lite, описывающий одну из разновидностей технологии цифровых абонентских линий (DSL — digital subscriber line), позволит продвинуть широкополосный доступ к Интернету на потребительский рынок.

В то же время, если производители оборудования DSL добьются своего, G.Lite заставит покупателей приобретать ПК с более быстрыми процессорами.

Значительную поддержку технологии G.Lite оказала Intel, к которой присоединились многие производители программного обеспечения, компьютеров, сетевого оборудования. Теперь очередь за владельцами сетей связи и Internet-провайдерами, которые должны внедрить G.Lite. Производители ПК планируют начать выпуск систем с поддержкой технологии в третьем квартале.

Некоторые компьютеры уже поддерживают G.Lite, но воспользоваться этим можно лишь при наличии специального ПО и доступности соответствующей услуги у провайдера.

Напомним, что G.Lite обеспечивает возможность постоянного высокоскоростного доступа к Интернету по стандартному медному телефонному кабелю параллельно с обычной голосовой связью без установки специальных делителей.

G.Lite позволяет передавать данные от пользователя к оператору на скорости до 512 Кбит/с, а в обратном направлении до 1,5 Мбит/с. Кроме того, G.Lite не подвержена недостаткам, свойственным при использовании обычного телефонного кабеля полноскоростной разновидности технологии DSL, не гарантирующей стабильности соединения.

Одно из серьезных достоинств G.Lite состоит также в возможности самостоятельной установки соответствующего оборудования самими пользователями на свои ПК без помощи специалистов технической службы телефонной компании или провайдера.

Учитывая это, у провайдеров есть все причины как можно скорее начать предоставление услуг G.Lite, которые обойдутся достаточно дешево как им самим, так и их клиентам. Во всяком случае, так дела обстоят в теории.

Насколько проста окажется инсталляция оборудования G.Lite на практике, до конца не понятно.

Во-первых, для G.Lite подходит не любое расположение телефонных розеток. Во-вторых, все компоненты G.Lite должны нормально взаимодействовать друг с другом.

Чтобы устранить все возможные недостатки до начала серийного производства, ряд компаний активно проводят испытания G.Lite в реальных условиях.

Подвид DSL подвергнут серьезному испытанию

То, что различные разновидности технологии цифровых абонентских линий (digital subscriber line — DSL) мало совместимы друг с другом, ни для кого не секрет. Но знаете ли вы, что G.Lite — подвид DSL, которому прочат наибольший успех, — не всегда совместим даже сам с собой?

Проблемы совместимости модемов G.Lite продолжались, пока технология не была стандартизована. Теперь поставщики оборудования могут, засучив рукава, взяться за обеспечение интероперабельности.

Производители модемов лихорадочно исправляют ошибки несовместимости, пытаясь добиться того, чтобы потребители могли заключать договор с любым поставщиком услуг G.Lite, не беспокоясь о типе купленного модема.

Большая часть трудностей была преодолена к началу решающего теста на совместимость — испытаний G.Lite Inter-operability Showcase, проходивших в июне в рамках выставки SuperCom в Атланте.

Впрочем, в испытаниях участвовали не все производители. Руководство некоторых компаний справедливо решило, что, даже если существующие модемы и смогли бы общаться друг с другом, скорости загрузки в 1,5 Мбит/с (предельной для G.Lite) достигнуть бы не удалось, как не удалось бы реализовать и поддержку требуемых для предоставления услуг DSL функций управления.

В частности, в G.Lite Inter-operability Showcase не приняла участия компания Paradyne, в которой считают, что результаты испытаний не оправдали затраченных усилий. Кроме того, окончательный вариант стандарта в любом случае не мог быть утвержден к моменту проведения экспозиции.

«Продемонстрированный уровень интероперабельности был всего лишь начальным. Кроме того, максимальная скорость достигнута не была», — отметил Фрэнк Винер, руководитель подразделения Paradyne, специализирующегося на оборудовании DSL.

Отчасти сложности с совместимостью связаны с тем, что работа над стандартом только-только завершена. Производители, которые уже выпускают оборудование G.Lite, в том числе наборы микросхем для модемов, до сих пор были вынуждены «стрелять по движущейся мишени». Если микросхемы не будут работать друг с другом, то и модемы тоже, в чем недавно получили возможность убедиться в 3Com.

3Com выпускает DSL-модемы для потребительского рынка на базе микросхем компаний Alcatel, Analog Devices и Texas Instruments, которые постоянно модифицируют ПО для этих микросхем, в результате чего производителю модемов очень трудно успевать с соответствующими обновлениями драйверов.

Поэтому было крайне важно, чтобы производители микросхем обеспечили хотя бы минимальную стабильность своих изделий. И действительно, интероперабельности своих микросхем добились компании Alcatel и Analog Devices. Теперь производители модемов также смогут сосредоточиться на решении проблем их совместимости.

Стремительное развитие G.Lite началось в январе 1998 года, когда группа компаний, в которую вошли Microsoft, Intel, Compaq и крупные американские операторы, приняла решение о скорейшей стандартизации технологии.

Группа получила название Universal ADSL Working Group (UAWG). Именно она выступила организатором июньских испытаний совместимости.

Российский рынок xDSL-устройств

Прежде чем приступить к обзору российского рынка xDSL-оборудования, необходимо уточнить, что он состоит из двух совершенно неравноценных сегментов — корпоративного и потребительского. Первый обслуживает операторов связи и корпоративных пользователей, живет относительно бурной жизнью и постепенно занимает все более заметную долю рынка телекоммуникационного оборудования.

Потребительский сегмент существует скорее виртуально. С одной стороны, вроде бы аппаратура, предназначенная для использования частными лицами, на российском рынке присутствует. Однако если даже единичные устройства этого класса и продаются, то они поступают опять же корпоративным пользователям. Короче говоря, реального потребительского сектора xDSL-оборудования в России не существует. Значительную роль в его оживлении может сыграть реализация проекта МГТС по построению сети передачи данных общего пользования (СПДОП).

Корпоративный сектор российского рынка xDSL-оборудования обслуживает главным образом нужды операторов общедоступных и ведомственных сетей. На оборудовании высокоскоростной цифровой абонентской линии (HDSL) и ее близкой родственницы для одной пары проводов (SDSL) строятся магистральные линии ведомственных сетей, организуются выносы абонентской емкости АТС, создаются линии подключения базовых станций сотовых и транкинговых сетей, земных станций спутниковой связи и точек присутствия Internet-провайдеров. Значительно реже xDSL-оборудование используется для подключения учрежденческих АТС (УАТС) и ЛВС организаций к сетям общего пользования. Ведь в России по-прежнему не так много компаний и организаций, которые могли бы арендовать у оператора каналы связи с быстродействием свыше 128 кбит/с, а с такой пропускной способностью справляются и другие, менее скоростные технологии.

Особенностью использования xDSL-оборудования в России является построение на нем магистральных линий связи длиной не менее 50, а то и более 100 км. По крайней мере, поставщики модемов Watson-4 Megatrans (производитель Schmid Telecom) и HiGain`98 (PairGain) утверждают, что это так. С некоторых пор крупные предприятия стали с помощью xDSL-оборудования объединять в единую ЛВС локальные сети своих подразделений.

Популярность оборудования цифровой абонентской линии в корпоративном секторе России несомненно возросла. Об этом можно судить хотя бы по числу участников семинаров, посвященных этой технологии.

Рост интереса к технологии обусловил выход на наш рынок новых производителей и стремительный рост числа поставщиков. В 1997 году на нем присутствовали десять производителей xDSL-оборудования. Сейчас их число возросло в десятки раз. Кроме уже упомянутых компаний есть еще много известных имен. Во-первых, стоит назвать компании, которые, по данным ИАЦ «Телекоммуникации», не покинули наш рынок — это 3Com, LG Information & Communications, Nokia Telecommunications, TAINET Communication System и Telindus. Во-вторых, за прошедшее время к ним прибавились Newbridge, Orckit, ADC Telecommunications. Наконец, среди производителей HDSL-устройств появился российский завод «Морион». Разработан продукт пермским НПО «Такт», завод же наладил серийное производство аппаратуры межстанционной связи с интерфейсом E1. На базе этой системы можно организовать тракт E1 протяженностью до 3,6 (при диаметре жилы 0,4 мм) или 13 (при 1,2 мм) км. На линии может быть установлено три регенератора, и тогда длина линии связи, надо полагать, увеличится втрое.

В российской системе применен комплект микросхем фирмы Level One Communications (сейчас — подразделение корпорации Intel), в котором используется линейный код 2b1q. По утверждению директора «Мориона» по маркетингу и сбыту Владимира Ардашева, их продукт — самый дешевый на рынке. Он совместим по мониторингу и управлению с аппаратурой ИКМ, поддерживает АТС «Квант» и передачу команд тарификации.

По оценке ИАЦ «Телекоммуникации», по-прежнему на российском рынке лидирует продукция швейцарской фирмы Schmid Telecom. НТЦ «Натекс», единственный дистрибутор этой компании, заявляет, что на базе оборудования семейства Watson в России установлено свыше 3 тыс. HDSL-линий. В этом году реселлером продукции Schmid Telecom стал еще один известный поставщик xDSL-оборудования — АО «Информсвязь».

По всей видимости, следующее место занимает продукция американской корпорации PairGain. Компания гордо заявляет, что по всему миру у нее установлено свыше 1 млн. xDSL-линий, однако умалчивает о том, какая доля из них приходится на Россию. Тем не менее ИАЦ «Телекоммуникации» располагает сведениями об инсталляции ее оборудования в Московском регионе и Приморском крае, в Башкирии и на Северном Кавказе, в Рязанской области и на Урале. Продукцию PairGain

продвигают в России компании ЮНИ, Diamond Communications, Race Communications и Step Logic.

Компания PairGain — один из трех производителей (наряду с Schmid Telecom и Nokia), первыми начавших поставлять на российский рынок xDSL-устройства. Пока соревнование выигрывает швейцарская фирма. Но если компанию Nokia это, по-видимому, устраивает (за исключением Северо-Западного региона активность ее в продвижении xDSL-устройств практически незаметна), то, судя по агрессивной стратегии PairGain, эта компания имеет серьезные намерения переломить ситуацию в свою пользу.

Не совсем ясна политика в области xDSL израильской компании RAD. У нее прочные позиции на рынке модемов для физических линий, она проводит рекламную кампанию своих устройств доступа в сети ATM, а вот особой активности на рынке xDSL не проявляет. Судя по всему, ее инсталляционная база за прошедший период времени значительно не увеличилась.

Из новичков на российском рынке следует выделить компании WaiLAN и RADWIZ. Один из сотрудников ИАЦ «Телекоммуникации» отметил появление на мировом рынке фирмы WaiLAN в апреле прошлого года. Обращает на себя внимание тот факт, что молодая компания заявила о себе представлением устройства для одной пары проводов с достаточно высокой дальностью связи при скорости 2 Мбит/с. Однако самое примечательное в устройстве AGATE 250 — механизм изменения линейной скорости (тактовой частоты), благодаря которому при ее снижении дальность связи по линии с диаметром жилы 0,5 мм увеличивается с 2,7 до 9 км. Как оказалось позже, этого производителя заметила и компания CompTek, которая решила дебютировать на российском рынке xDSL-оборудования именно с продукцией WaiLAN.

На выставке Internetcom компания CompTek продемонстрировала еще одно прямо-таки уникальное устройство производства WaiLAN. Система с изменяемой линейной скоростью передачи AGATE 850 способна передавать данные по двум парам телефонного кабеля со скоростью 7 Мбит/с (в обе стороны) на расстояние около 3,5 км. Каждый модем снабжен двумя портами E1, двумя синхронными портами V.35 и одним портом Ethernet для подключения к локальной сети. Это устройство (цена с НДС составляет 2790 долл.) предназначено для построения действительно высокоскоростных корпоративных сетей, способных обеспечить передачу мультимедийной информации (данных, видео и телефонного трафика).

Как объяснил технический директор CompTek Петр Кочегаров, весь фокус заключается в том, что в модеме размещено по два ADSL-бло-

ка. Каждый блок работает по одной паре как обычное асимметричное устройство со скоростью 6 Мбит/с в одну сторону и 1 Мбит/с в другую. Фактически модем AGATE 850 функционирует как инверсный мультиплексор. Передающий модем разделяет поступающий на его вход 7-Мбит/с поток на два (6+1 Мбит/с) и передает их по разным парам. Принимающий модем суммирует два входящих потока и выдает дальше опять 7 Мбит/с. К недостаткам RADSL-модема AGATE 850 и сходного с ним AGATE 800 можно отнести отсутствие поддержки маршрутизации; они являются обычными прозрачными мостами.

Еще одной интересной новинкой российского рынка стала система IPTL израильской компании RADWIZ. На российском рынке ее предлагает компания «Омнибэнд Групп». Это SDSL-система, т. е. она работает по одной паре проводов и ориентирована главным образом на использование в сетях телефонных операторов и поставщиков услуг Интернета. IPTL обеспечивает как передачу данных, так и обычную и пакетную (IP) телефонную связь. Абонентский модем системы IPTL имеет встроенный маршрутизатор и межсетевой экран, а также поддерживает протоколы DHCP и NAT. К четырем его портам можно подключить компьютеры, ЛВС и телефонные аппараты в любой комбинации.

Устанавливаемый на телефонной станции концентратор поддерживает шесть абонентских линий и имеет 12 аналоговых портов и три порта E1 для подключения к местной АТС. Каждая абонентская линия обеспечивает передачу информации со скоростью до 2 Мбит/с на расстояние до 2 км. В состав системы IPTL входят платформно-независимые средства дистанционного управления, позволяющие осуществлять контроль и администрирование системы через Интернет (например, устанавливать необходимую пользователям скорость передачи данных или требуемый уровень качества обслуживания).

Продолжается падение цен (правда, в долларах) на xDSL-оборудование. Особенно заметно снижение цен на устройства организации 2-Мбит/с трактов.

Перспективы ADSL

В конце 80-х годов поставщиков телекоммуникационных услуг захватила идея использовать технологию DSL для предоставления различного видеосервиса по имеющимся у телефонных компаний в избытке медным абонентским парам. Немногим позже, в начале 90-х, корпорация Bell Communications Research, или просто Bellcore (тогда — исследовательский центр региональных телефонных компаний США, а с марта этого года — дочернее предприятие Telcordia компании Science Applications International) опубликовала первые спецификации технологии

асимметричной цифровой абонентской линии (ADSL). Уже в 1993 г. операторы Bell Atlantic и British Telecom приступили к испытаниям соответствующего оборудования.

После более чем четырехлетних попыток воплотить в жизнь свою мечту североамериканские (именно на этом континенте происходили более-менее крупные испытания) операторы поняли, что на видеоуслугах денег не заработаешь. В 1998 г. американцы начали массовое развертывание ADSL-услуг, но на сравнительно низких скоростях (от 128 кбит/с до 1,5 Мбит/с) и почти исключительно для передачи данных, включая доступ в Интернет.

В остальном мире (за исключением Гонконга и Сингапура) до массового предложения DSL-услуг дело так и не дошло. Не в последнюю очередь это связано с тем, что там по-прежнему пытаются приспособить DSL под видеосервис. Есть все основания полагать, что однажды, подобно своим североамериканским коллегам, европейцы осознают бесперспективность этого направления и займутся делом — предоставлением доступа в транспортные сети и Интернет.

Для нас не было неожиданностью, что первыми в Старом Свете опомнились немцы. Deutsche Telekom приступил к испытаниям ADSL в Нюрнберге в декабре 1996 г. и планировал начать предоставление соответствующих услуг на коммерческой основе в 1998 г. ADSL-аппаратура была установлена на одной из нюрнбергских АТС и в 100 квартирах. Главный упор делался на видеоуслуги. Участникам испытаний предлагалось заказывать на свои компьютеры трансляцию информационных программ региональных телевизионных каналов N-TV, Баварского и Южно-Германского телевидения, а также Института научного фильма. В нюрнбергском издательстве Hans Mueller & Co. можно было заказать трансляцию местных новостей. Кроме того, предлагалось в интерактивном режиме делать покупки в фирме Quelle. Передача видеоматериалов осуществлялась с помощью видеосерверов фирмы Ncube и ПО компании Oracle.

В марте 1998 г. вместо предоставления коммерческих услуг Deutsche Telekom приступил к новому этапу тестирования в Северном Рейне-Вестфалии — самой густо населенной федеральной земле Германии. Однако видеосервис уже почти не упоминался. Вторая попытка была нацелена на исследование возможности применения ADSL в сфере среднего и малого бизнеса, в первую очередь для обеспечения высокоскоростного доступа в Интернет, а также в издательском деле, медицине и образовании. Кроме того, участникам эксперимента (около 100 корпоративных и 350 индивидуальных пользователей) предлагалось до конца года вволю наслаждаться компьютерными играми и опять же совершать

покупки в электронных магазинах. Коммерческое обслуживание было перенесено на начало 1999 г. и за один год планировалось охватить в 40 крупнейших городах Германии 100 тыс. абонентов, до 2003 г. — 80% населения страны. Уже тогда стало ясно, что частные лица не смогут оплачивать скорости более 1,5 Мбит/с, а для корпоративных клиентов планка была установлена на уровне 8 Мбит/с.

Программа этого этапа испытаний предусматривала доступ в Интернет частных пользователей с помощью ADSL-модемов, а мультимедийный сервис ограничивался предложением на серверах службы T-Online музыкальных видеоклипов, трехмерных анимационных роликов и мультимедиа-игр. Корпоративные пользователи применяли ADSL-модемы для удаленного доступа в сети своих предприятий и организаций, для видеоконференцсвязи и объединения локальных сетей. О видео по запросу ни слова.

В конце апреля 1999 г., после многочисленных задержек в пути, поезд ADSL наконец-то прибыл в Германию. Но не для всех. На него могли попасть только корпоративные пользователи в восьми крупнейших городах: Берлине, Бонне, Гамбурге, Дюссельдорфе, Кельне, Мюнхене, Франкфурте-на-Майне и Штуттгарте. Как и следовало ожидать, им был предложен доступ в Интернет, транспортные сети и ЛВС их фирм. При этом максимальное быстродействие прямого канала (от узла провайдера к абоненту) было снижено на 2 Мбит/с и составило 6 Мбит/с, в обратном канале предложены скорости от 160 до 576 кбит/с. ADSL-сервисом можно воспользоваться в двух вариантах: в рамках служб T-Interconnect и T-Net-ATM.

Тарифы службы T-Interconnect официально не объявлялись. Известно лишь, что взимается единовременная плата за установку канала, а абонентская плата начисляется в зависимости от средней полосы пропускания.

В рамках службы T-Net-ATM предложено два варианта доступа: ATM-Access и ATM-Solution. В первом случае владельцы ADSL-устройств могут пользоваться коммутируемыми виртуальными каналами (SVC). Услуга ATM-Solution предполагает использование как SVC, так и постоянных виртуальных каналов (PVC) в ATM-сеть Deutsche Telekom. Быстродействие ADSL-соединений составляет в прямом канале от 2 до 6,144 Мбит/с, в обратном — от 204 до 614 кбит/с. Расценки соответствуют тарифным планам службы T-Net-ATM и включают плату за установку, ежемесячную абонентскую плату и повременку.

Представители Deutsche Telekom обещают, что и индивидуальные пользователи в вышеназванных городах смогут испытать Fast Internet. Им будут предложены два тарифных плана: Speed-50 и Speed-100. Они

различаются не скоростью (в обоих случаях она составляет вниз 768 и вверх 128 кбит/с), а количеством «бесплатных» часов пользования Интернет. Подписчики Speed-50 получают за абонентскую плату 50 таких часов в месяц, абоненты Speed-100 — 100 часов. Но это — плата только за доступ в Интернет. А еще частный пользователь должен будет вносить за объединенную линию ISDN/ADSL ежемесячную плату (обычная линия ISDN BRI стоит в два раза дешевле) и платить повременку за ISDN-звонки.

Планируемые расценки для частных пользователей, по мнению аналитика Gartner Group Сьюзен Томсон, отпугнут многих потенциальных потребителей ADSL-доступа. Поэтому она очень скептически относится к тому, что Deutsche Telekom думает приобрести в этом году 100 тыс. абонентов. Тем не менее Томсон признает, что в отсутствие реальной конкуренции вряд ли стоит рассчитывать на скорое снижение цен. Действительная же конкуренция в области ADSL-сервиса возможна только с падением цен на прямые провода.

Всем уже, наверное, известно, что в течение ближайших двух лет МГТС планирует на базе своей абонентской телефонной сети и сети ATM дочерней компании «Голден Лайн» создать СПДОП. Реализация этого проекта потребует от МГТС на всех своих АТС установить мультиплексоры цифровых абонентских линий, частично заменить кабельное хозяйство абонентской сети и, главное, убедить москвичей в необходимости приобретения ADSL-модемов. Будем надеяться, что с первыми двумя задачами МГТС если и не полностью, то в основном справится. В противном случае руководству компании будет трудно отчитаться за средства, полученные от размещения евробондов. Ведь одним из двух проектов, под которые зарубежные финансовые институты давали деньги, как раз и была СПДОП (второй проект — построение интеллектуальной сети).

Значительно труднее осилить третью задачу. Во-первых, даже если и можно будет приобрести встраиваемые модемы Cisco 605 за 227 долл., вряд ли 5 тыс. москвичей (в первый год предоставления услуг СПДОП столичный оператор рассчитывает именно на такое число пользователей) захотят это сделать в условиях перманентных финансовых кризисов и по причине того, что это устройство не позволяет одновременно использовать линию для обычного телефонного разговора. Все же остальные ADSL-модемы стоят значительно дороже.

Во-вторых, чем МГТС собирается привлекать пользователей ADSL-услуг? В США абонентам предлагают достаточно скоростной доступ (свыше 128 кбит/с) за цену, в два-три раза превышающую стоимость доступа с помощью обычного модема. В московском варианте это может

означать приблизительно 3 долл./ч или порядка 100–120 долл./мес без ограничения времени доступа. Много ли найдется желающих — большой вопрос. И какой, собственно, скоростной доступ сможет предложить МГТС? Сколько потребуется владельцев ADSL-устройств, чтобы напрочь забить 100-Мбит/с полосу всех российских каналов в зарубежную часть Интернет и 155-Мбит/с мощь ATM-сети «Голден Лайн»? Все это смешно сравнивать с пропускной способностью американских сетей. Даже Deutsche Telekom уже перевел свою ATM-сеть на 622 Мбит/с, а до конца года собирается довести полосу пропускания до 2,4 Гбит/с.

МГТС и «Голден Лайн», не веря опыту американцев и немцев, намерены изыскать потребителей «видео-по-запросу» (в списке МГТС эта услуга стоит на втором месте, у «Голден Лайн» — на третьем) и зрителей программ РТР и «Вести» (второе место в списке «Голден Лайн»). МГТС, кроме того, мечтает осчастливить население телевидением высокой четкости и ТВ-вещанием в формате MPEG. Остается надеяться на то, что другие российские операторы, которые пойдут вслед за МГТС, на эти грабли больше не наступят.

Есть в списках МГТС и «Голден Лайн» услуга организации виртуальных частных сетей (VPN). Из разговоров с представителями обеих компаний можно понять, что пока не существует точных расчетов, как этот сервис повлияет на бизнес той же «Голден Лайн» и других компаний, подконтрольных холдингу «Система Телеком», связанный с предоставлением выделенных каналов. Ряд иностранных экспертов полагает, что технология ADSL не является настолько зрелой, чтобы обеспечить высококачественные услуги VPN. Один из сотрудников компании «Реллайн» (он пожелал остаться неназванным), принимавший участие в опытах МГТС и «Голден Лайн», полностью согласился с этой точкой зрения. По его словам, тестировавшиеся мультиплексоры цифровых абонентских линий как минимум раз в неделю «падают», для восстановления их работы необходим выезд специалиста, это требует как временных затрат, так и значительного отвлечения людских ресурсов. Кроме того, система управления сети «Голден Лайн» не позволяет дистанционно управлять не относящимися к линейке продуктов Newbridge мультиплексорами и абонентскими DSL-устройствами. Надо полагать, задачи по организации VPN на сегодняшний день лучше оставить за традиционными средствами доступа по выделенным линиям, каналам ISDN, frame relay и ATM (в том числе организованным с помощью проверенных временем HDSL-устройств). Хотя, возможно, придется заключать с клиентами более жесткие договоры об уровне обслуживания (SLA), чтобы они остались верны прежним технологиям и не подорвали сложившийся бизнес операторов.

Сетевым администраторам и руководителям предприятий, подумывающим о переходе на ADSL-технологию, следует также иметь в виду, что абонентское ADSL-оборудование разрабатывалось и производится с прицелом на массовый потребительский рынок. Часто оно стоит дешевле устройств доступа к сетям frame relay и ATM, HDSL- и SDSL-модемов, а также профессиональных (употребим слово, которое используется для обозначения аналоговых модемов, превосходящих по классу бытовые устройства) RADSL- и ADSL-модемов, поскольку не предназначено для решения задач, от которых зависит финансовое состояние предприятия или качество услуг оператора сети общего пользования.

Но давайте закончим со списком услуг, которые МГТС собирается предложить пользователям СПДОП. Неназванными пока остались:

- работа на дому;
- IP-телефония и как частный вариант Internet-телефония;
- охранная сигнализация и наблюдение;
- электронная коммерция и покупки с помощью компьютера;
- телеобучение;
- сетевые мультимедийные конференции;
- телемедицина;
- интерактивные игры;
- целевая реклама;
- поддержка и обслуживание клиентов.

Мне кажется, что из этого списка только четыре услуги однозначно можно отнести к сервису потребительского класса: работу на дому, Internet-телефонию, покупки с помощью компьютера и интерактивные игры. При относительно низких тарифах (не более 50 долл. за неограниченный по времени доступ) и без дополнительной оплаты доступа к соответствующим ресурсам они могли бы пользоваться спросом.

Владельцам и операторам ресурсов электронной коммерции (проще говоря, Internet-магазинов), телеобучения, телемедицины и IP-телефонии, а также компаниям, придающим значение качественной поддержке и обслуживанию клиентов, возможно, по вышеназванным причинам пока не стоит связываться с ADSL-технологией или, во всяком случае, очень тщательно выбирать профессиональный ADSL-модем и обязательно заключить с МГТС договор об уровне обслуживания.

Отдельно стоит сказать о сервисе мультимедийных конференций. Почему-то многие уверены, что его можно предоставлять только с помощью изначально симметричных технологий передачи данных, включая, например, HDSL и SDSL. При этом упускается из виду, что часто для качественной видеоконференции достаточно полосы в 384 кбит/с, а ADSL-устройства обеспечивают в обратном канале (более «медленном») скорости как минимум вдвое выше. Кроме того, абсолютное большинство асимметричных DSL-устройств можно сконфигурировать для работы в симметричном режиме, например с быстродействием в прямом и обратном каналах 768 кбит/с или 1 Мбит/с.

Еще раз о G.Lite

МГТС сделал в пользу полноформатной версии ADSL. Одна единственная положительная сторона такого выбора (при условии, что действительно взят курс на массовую услугу) вот-вот перестанет быть таковой. Она состоит в том, что соответствующее оборудование уже прошло проверку на жизнеспособность в различных сетях земного шара. Во всем остальном при ориентации на массовый и относительно недорогой сервис ADSL проигрывает облегченной версии G.Lite, окончательный стандарт на которую должен быть принят МСЭ со дня на день. Основными преимуществами G.Lite (рекомендация G.992) являются.

Меньшая стоимость оборудования, в том числе за счет отказа от частотного разделителя, который стоит около 100 долл.

Производители и операторы, проведшие испытания подобных устройств, чуть ли не в один голос утверждают, что модем или модемную плату G.Lite пользователь может инсталлировать и запустить в работу сам (для подключения ADSL-модема и частотного разделителя требуется выезд специалиста на место.

Отсутствие лишней коробки обусловливает простоту и низкую стоимость обслуживания (вернее, модем G.Lite, как и обычный аналоговый модем, практически не требует никакого обслуживания).

Производители твердо обещают с принятием окончательных спецификаций G.992 сразу же начать серийный выпуск стандартных и взаимосовместимых устройств. Поскольку МГТС собирается приступить к предоставлению услуг СПДОП не раньше 2001 г., есть время еще раз оценить сделанный выбор. Начальник исследовательского центра МГТС Владимир Беленкович, выступая на семинаре, организованном компанией Diamond Communications, обосновал отсутствие в МГТС размышлений по поводу G.Lite тем, что никто московской телефонной сети такого оборудования не предлагал. «Если бы оно существовало в природе, — добавил он, — то его, несомненно, предложили бы МГТС». Неужели он не знает, что совместимое с предварительным стандартом оборудование есть у Orckit, чьи устройства наряду с устройствами Cisco МГТС предполагает (на сегодняшний день) устанавливать в своей СПДОП. Интересно, почему руководство Orckit компаниям GTE и Deutsche Telecom предложило протестировать свое G.Lite-совместимое оборудование, а МГТС — нет?

У сторонников ADSL есть еще один аргумент — скорость. ADSL-модемы теоретически могут разгоняться на прием до 8 и на передачу до 1,5 Мбит/с. Максимальное быстродействие их более легких соперников — 1,5 Мбит/с (скорость передачи еще ниже). Хотелось бы знать, сколько в Москве найдется частных пользователей, которым по карману будут каналы хотя бы в 1,5 Мбит/с. Напомним, что в США ADSL-услуга на скорости 768 кбит/с стоит дороже 100 долл. в месяц. Там считается, что более высокие скорости могут понадобиться только корпоративным пользователям. По-видимому, это знают и в МГТС, раз г-н Беленкович заявил, что массовому московскому пользователю будут предлагаться услуги с быстродействием 128–256 кбит/с, т. е. скоростями, с которыми устройства G.Lite справляются без всякого труда.

Часть 4. Собери свой жучок

Введение

Мы живем в век интерактивных технологий, когда информация стала самым дорогим товаром. Сейчас, дабы получить необходимые сведения, в ход пускают любые средства, так как от оперативности зависит слишком многое. Теперь установка разнообразной прослушивающей аппаратуры не является привилегией разведки и правоохранительных органов — это может сделать каждый...

Речь идет о способах скрытого прослушивания помещений с применением технических средств. Как правило, оно осуществляется с помощью телефона, направленных и контактных микрофонов и разнообразных радиозакладок. Несмотря на то, что Конституция РФ (гл.2, ст. 23) допускает ограничение права гражданина на неприкосновенность частной жизни только с санкции суда, этот принцип повсеместно нарушается. Виной тому, как повышенная криминализация нашего общества, так и вытекающая из нее потребность граждан в самозащите от возможных посягательств.

Было бы неверным утверждать, что прослушивающие устройства являются детищем нашего времени желание узнать чужие тайны лежит в природе человека. Если до XX века профессионалам и любителям от шпионажа приходилось довольствоваться перлюстрацией писем и потайными комнатами, позволявшими незримо присутствовать при интересном разговоре, то с возникновением совершенных технических средств поле их деятельности стало поистине огромным. Впервые о «жучках» громко заговорили в 1972 году в США, когда группа «активистов» при содействии представителей предвыборного штаба президента Никсона тайно проникла в штаб-квартиру кандидата от Демократической партии, расположенную в вашингтонском отеле «Уотергейт». Не найдя интересных бумаг, взломщики оставили в помещении несколько радиомикрофонов, желая знать, о чем говорят конкуренты по выборам. Итог известен — дело получило скандальную огласку, а президент Никсон был вынужден уйти в отставку. Так «жучки» перешли из арсенала разведки в разряд методов политической и корпоративной борьбы — это стало началом эры частного сыска.

Сейчас прослушивание чужих разговоров доступно всем: никакие сложные технологии при изготовлении миниатюрных микрофонов не используются, и любой мало-мальски грамотный специалист сможет собрать такой аппарат за несколько часов. Основным техническим средством прослушивания уже много лет остается обыкновенный радиомикрофон, изменяются только его размеры, причем главной особенностью каждой конкретной модели микрофона является способ маскировки. Основная тенденция последних лет заключается в миниатюризации всей полупроводниковой техники. Наиболее широко для получения информации о содержании бесед в закрытом помещении используются перечисленные ниже средства.

Телефонные «жучки»

Эти встроенные в телефон устройства предназначены передавать беседы, проводимые в закрытой комнате при положенной на рычаг трубке через телефонную линию. Слушать удается как ведущиеся телефонные переговоры, так и все беседы, ведущиеся в комнате, при положенной на рычаг трубке. К приемам, ориентированным на последнее, относятся: слушание через звонковую цепь, внутрикомнатное прослушивание с применением высокочастотной накачки, встраивание «жучка», активизируемого по коду через удаленный телефон, встраивание в аппарат «жучка», временно блокирующего рычаг трубки в ходе опускания ее после ответа на обычный телефонный звонок.

Телефоны при наружной активации

В данном случае в отличие от телефонных «жучков», встраиваемых в аппарат, к контролируемому телефону даже не прикасаются руками. Информация снимается с телефонной линии при лежащей на рычаге трубке путем внешней активации высокочастотными колебаниями ее микрофона, а порой и через перехват микротоков, появляющихся в электромагнитном звонке при легчайших сотрясениях его подвижных частей. Следует сказать, что сходным образом можно перехватывать полезные микроэлектротоки не только с телефонного, но и с квартирного звонка.

Радиожучки

Это микропередатчики УКВ-диапазона, которые могут быть и стационарными, и временными. Стационарные модели питаются от электрической сети и обычно размещаются в торшерах, телевизорах, электророзетках, люстрах и других стандартных элементах обстановки. Все временные приборы закладываются при тайном или легальном посещении объекта (посетителями, уборщицами и т. п.) в места, где их будет

трудно обнаружить (за книги, среди бижутерии, в обивке мебели...) и нередко маскируются под шариковые ручки, коробки от спичек, безделушки и прочие малозаметные вещицы.

Главным недостатком большинства данных конструкций является ограниченный — от десятков до нескольких сотен часов — период их автономной работы, в частности зависящий от излучаемой в пространство мощности и электроемкости используемых батарей. Сами разговоры перехватываются на расстоянии от 5 до 30 метров, тогда как радиус передачи информации составляет от десятков и до сотен метров, причем для увеличения дальности применяют промежуточные ретрансляторы, а «жучки» иной раз устанавливают на металлические предметы — трубы водоснабжения, радиаторы отопления, бытовые электроприборы (они служат дополнительной передающей антенной).

Фирменные радиозакладки работают на самых разных частотах, от десятка и до тысячи МГц, но для импортных образцов наиболее характерно вклинивание в диапазоны 20–25 МГц, 130–174 МГц, 400–512 МГц. Повышение рабочей частоты увеличивает дальность действия в бетонных зданиях, но здесь требуются специальные радиоприемники либо преобразующие приставки (конвертеры) к бытовым УКВ-приемникам. Подстраховываясь от случайного обнаружения, профессионалы иной раз задействуют такие уловки, как необычное растягивание спектра передаваемого сигнала, сдвоенную модуляцию несущей частоты, уменьшение исходной мощности с применением промежуточного ретранслятора, и другие подобные приемы.

Стационарные микрофоны

Такие устройства маскируются в самых неожиданных местах контролируемого пространства и соединяются тончайшими проводниками с создаваемым неподалеку пунктом прослушивания. Отличными микрофонами могут служить ДСП-плиты столов, шкафов и книжных полок с жестко приклеенными к ним пьезо-кристаллами. Тоненькие провода протягиваются под обоями, либо в плинтусах и обычно покидают комнату вместе с телефонной или радиотрансляционной линией. Явным недостатком тут является необходимость предварительного проникновения в намечаемое помещение при довольно долгом — вплоть до нескольких часов — прерывании там, хотя иной раз подобное удается обеспечить, к примеру, под предлогом ремонта.

Сетевые передатчики

Они действуют в низкочастотном (50–3000 кГц) волновом диапазоне, встраиваются в электроприборы, а как линию активной связи ис-

пользуют провода электропроводки. Отловить передаваемый сигнал можно из любой соседней электророзетки, однако первый силовой трансформатор надежно блокирует всю последующую передачу.

Подведенные микрофоны

Все эти подсоединяемые к усилителю микрофоны могут иметь самую разнообразную конструкцию, соответствующую «акустическим щелям», обнаруженным в интересующем помещении. Динамический тяжелый капсюль, например, можно опустить в вентиляционную трубу с крыши, а плоский кристаллический микрофон подвести под дверь снизу. При отсутствии подобных лазеек используются электрические розетки, которые в смежных комнатах иной раз бывают спарены. Снятие защитной коробки с одной из них открывает доступ к другой, а через нее — в близлежащее помещение. Иногда имеет смысл просверлить в стене микроотверстие, не заметное для чужого глаза, или воспользоваться замочной скважиной. Для таких изощренных вариантов существует специфический тонкотрубковый, или «игольчатый» микрофон, звук к которому подводится через тонкую трубку длиной сантиметров в тридцать.

Контактный микрофон

В качестве подобного устройства превосходно работает заурядный медицинский стетоскоп, спаренный (чтобы повысить восприимчивость) с подходящим микрофонным капсюлем, который подсоединен к чувствительному усилителю. В простых случаях, конечно, можно обойтись и одним стетоскопом без какой-либо электроники.

Очень качественные контактные датчики получаются из пьезокерамических головок от проигрывателей либо из стандартных пьезоизлучателей — электрических часов, звуковых игрушек, сувениров и телефонов. Так как данные устройства засекают микроколебания контактных перегородок, требуется весьма тщательно выбирать место их приложения, зависящее от конструктивных особенностей конкретной стены. В некоторых случаях имеет смысл крепко приклеить пьезоэлемент к доступной стороне стены или к наружному стеклу рамы. Превосходный акустический сигнал иной раз удается снимать с труб водоснабжения батареи отопления.

Импровизированные резонаторы

Перехватывать переговоры в смежном помещении часто удается и без спецаппаратуры, прибегая к помощи случайно оказавшегося под рукой питейного бокала (или рюмки), ободок которого плотно прижимается к стене, а донышко (торец ножки) — вплотную к уху. Возникающий

при этом звук сильно зависит как от состояния и структуры стены, так и от конфигурации прибора и материала, из которого он изготовлен (лучше — хрусталь).

Наряду с указанными выше существуют и другие варианты подслушивания, применяющие, к примеру, посылаемые дальним выстрелом «радиопули», модуляцию лазерного луча микровибрациями оконного стекла, перехват побочных электромагнитных излучений бытовой радиоаппаратуры, бесконтактную активацию пассивных микроволновых излучателей... Все эти методики, впрочем, профессионально сложны и не рекомендуются для импровизированного применения.

Большинство из перечисленных средств легко как изготовить, так и приобрести. Хотя фирмы — производители подобной аппаратуры обязаны иметь лицензию ФСБ и Гостехкомиссии РФ, а за ее продажу лицам, не имеющим права на использование подобной техники, продавцу, согласно ст. 138 гл. 19 УК РФ, грозит заключение на срок до трех лет лишения свободы.

Зато, чтобы создать «жучок» самому, кроме большого желания, не надо почти ничего. Схемы лучше взять из нескольких книг (серия книг «Шпионские штучки») или из Интернета и разобраться в них самому. В книгах очень много ошибок и, дай бог, чтобы каждая вторая схема работала.

Детали лучше всего заказывать по каталогу из Германии: выбор огромный, разброс цен тоже. И еще один минус — надо 2–4 недели ждать получения заказа. Если вы точно уверены в правильности схемы, то сразу покупайте SMD детали (очень маленькие размеры), если — нет, то лучше сначала собрать схему на нормальных деталях, а потом перенести на плату.

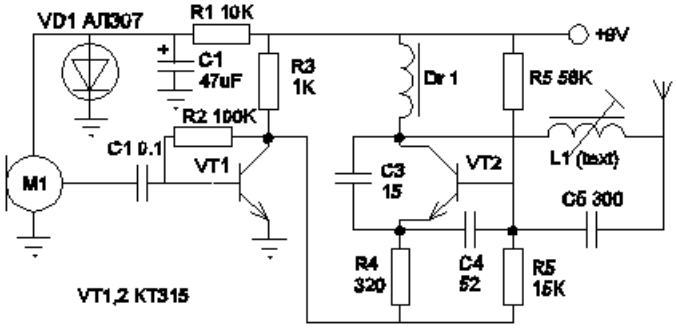
Что касается батареек, то, в принципе, их можно купить в любом ларьке.

Радиомикрофон АМ 27 MHz (~ 100 m)

Радиомикрофон представляет из себя АМ передатчик с дальностью действия около 100 метров.

Передатчик состоит из генератора высокой частоты, собранного на транзисторе VT2, и однокаскадного усилителя звуковой частоты на транзисторе VT1. На вход последнего через конденсатор C1 поступает звуковой сигнал от микрофона M электретного типа (МКЭ-3 или «сосна»). Нагрузку усилителя составляют резистор R3 и генератор высокой

частоты, включенный межу плюсом питания и коллектором транзистора VT1. С усилением сигнала напряжение на коллекторе VT1 изменяется, что приводит к амплитудной модуляции сигнала несущей частоты передатчика, излучаемого антенной.



Катушка L1 намотана на каркасе из полистирола диаметром 7 мм. Она имеет подстроечный сердечник из феррита 600 НН диаметром 2.8 мм и длиной 12 мм. Катушка содержит 8 витков провода ПЭВ 0.15 мм, намотанного виток к витку. Дроссель ДПМ-01 100 uH или намотан на резисторе МЛТ 0.5 с сопротивлением более 100 кОм и содержит 80 витков провода ПЭВ 0.1 мм виток к витку. В качестве антенны используется стальной упругий провод диной 20 см.

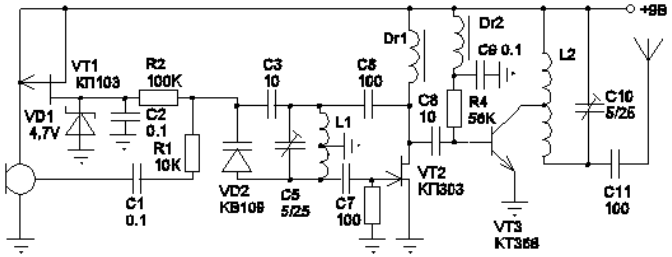
При настройке частоту устанавливают вращением сердечника в катушке L1. После регулировки его закрепляют каплей парафина.

Радиомикрофон ЧМ 65...108 MHz

Этот передатчик при скромных габаритах позволяет передавать информацию на расстояние до 300 метров. Прием сигнала может вестись на любой приемник УКВ ЧМ диапазона. Для питания подходит любой источник с напряжением 5...15 вольт.

Задающий генератор выполнен на транзисторе КП303. Частота генерации определяется элементами L1, C5, C3, VD2. Частотная модуляция осуществляется путем подачи модулирующего напряжения звуковой частоты на варикап VD2 типа КВ109. Рабочая точка варикапа задается напряжением, поступающим через резистор R2 со стабилизатора напряжения. Стабилизатор включает в себя генератор стабильного тока на полевом транзисторе VT1 типа КП103, стабилитрон VD1 типа КС147А и конденсатор C2.

Усилитель мощности выполнен на транзисторе VT3 типа КТ368. Режим его работы задается резистором R4. В качестве антенны используется кусок провода длиной 15...20 см.



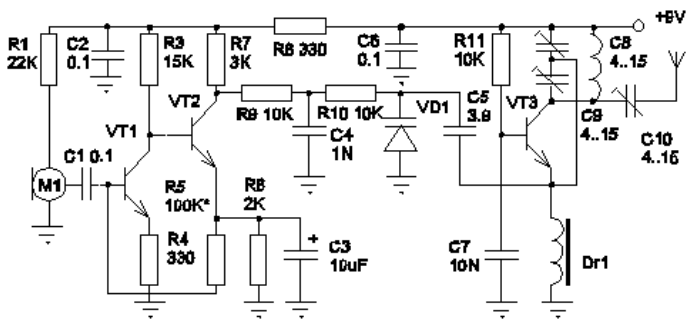
Дроссели Dr1 Dr2 могут быть любые индуктивностью 10...150 uH. Катушки L1 и L2 наматываются на полистироловых каркасах диаметром 5 мм с подстроечными сердечниками 100ВЧ или 50ВЧ. Количество витков — 3.5 с отводом от середины, шаг намотки 1 мм, провод ПЭВ 0.5 мм. Вместо КП303 подойдет КП302 или КП307.

Настройка заключается в установке необходимой частоты генератора конденсатором C5, получения максимальной выходной мощности путем подбора сопротивления резистора R4 и подстройке резонансной частоты контура конденсатором C10.

Радиомикрофон большой мощности

При использовании компактной антенны это устройство обеспечивает дальность связи около 100 метров, а при использовании полноразмерной штыревой антенны — более 600 метров.

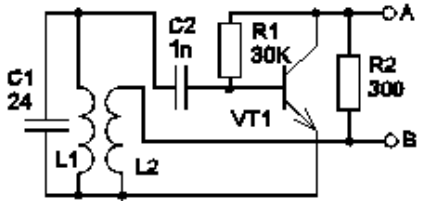
Сигнал от микрофона поступает на усилитель низкой частоты (транзисторы VT1, VT2) с непосредственными связями. Усиленный сигнал через фильтр R9, C4, R10 подается на варикап VD1 типа КВ109, включенный в эмиттерную цепь транзистора VT3 типа КТ904. Напряжение смещения варикапа задается коллекторным напряжением транзистора VT2. Генератор ВЧ выполнен по схеме общей базы. В коллекторной цепи транзистора VT3 включен контур C8, C9, L1. Частота настройки определяется индуктивностью катушки и емкостями C8, C5, VD1. Конденсатор C9 устанавливает глубину обратной связи, а C10 — согласование с антенной.



Дроссель любого типа индуктивностью около 60 uH. Катушка L1 — бескаркасная, с внутренним диаметром 8 мм, имеет 7 витков провода ПЭВ 0.8 мм. Длина полной антенны 0.75...1 метр. Мощность передатчика около 200 мВт. Если такая мощность не нужна, можно понизить ее, применив резистор R2 сопротивлением 50..100 кОм и заменив дроссель резистором сопротивлением около 300 Ом. Транзистор при этом можно заменить на КТ368. Стабильность частоты маломощного передатчика выше, и увеличивается срок службы батарей.

Телефонный микропередатчик

Генератор микропередатчика выполнен на высокочастотном транзисторе VT1 прямой проводимости типа КТ361, между базой и эмиттером которого включен контур C1,L1. Катушка L2 служит для связи с линией, которая в данном случае играет роль антенны.

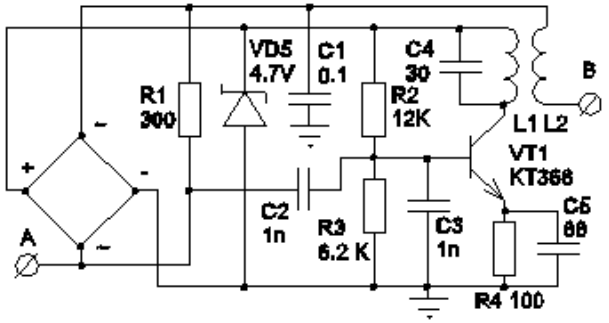


Недостатками данного устройства являются небольшой радиус действия и наличие сетевого фона вследствие отсутствия стабилизатора напряжения. Однако эти недостатки компенсируются исключительной простотой и дешевизной данного устройства. Катушка L1 содержит 4...6 витков провода ПЭВ 0.5 мм на диаметре 6 мм для диапазона 65...108 MHz.

Передатчик включается в разрыв телефонной линии.

Телефонный ЧМ передатчик

Ниже предлагается усовершенствованная схема телефонного радиопередатчика с использованием телефонной линии в качестве антенны и имеющего стабилизатор напряжения. Это позволяет почти полностью устранить сетевой фон.



Устройство можно закамуфлировать под телефонную розетку, конденсатор, распаечную коробку. Катушку L1 наматывают на оправке диаметром 6 мм проводом ПЭВ 0.5 мм. Она содержит около 6 витков. L2 расположена поверх нее и имеет 3 витка того же провода. Возможно изготовление катушек прямо на плате печатным способом. При этом используется двухсторонний стеклотекстолит, а катушки для обеспечения связи располагают одна над другой.

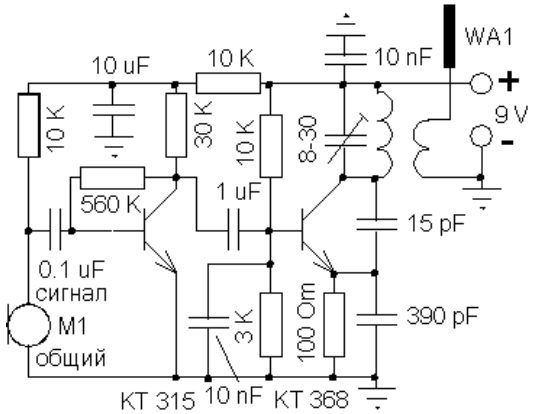
Передатчик включается в разрыв телефонной линии.

Жучок

На рисунке ниже приводится схема. Собирал ее много раз, из самых разных деталей и она всегда классно работает. Номиналы деталей некритичны и могут отличаться в ту или иную сторону в полтора раза. Я принимал сигнал этого жучка, работающего в комнате ж/б дома на расстоянии около 300 м при отсутствии прямой видимости на приемник плейера.

Чувствительность по НЧ позволяет прослушивать громкий разговор в комнате. Если же тракт НЧ дополнить еще одним каскадом усиления, то становится слышим даже тихий шепот... Правда, от громкой речи схема тогда перегружается и бы надо еще ставить АРУ. Если же вам

требуется передатчик — радиомикрофон (когда вы планируете непосредственно бубнить прямо в микрофонный капсюль), то каскад усиления НЧ вообще не нужен.



Микрофон — телефонный электретный капсюль (применяется также в магнитофонах). На задней плате есть два контакта, один из них соединен с корпусом микрофона. Это минусовой вывод — общий. На второй контакт подается питание через резистор 5...20 кОм. Если усиление слишком велико, в цепь эмиттера первого транзистора включите сопротивление 100 Ом...10 кОм. Резистор в цепи эмиттера второго транзистора определяет рабочий ток генератора ВЧ. Не уменьшайте его значение ниже 50 Ом — транзистор будет перегружен. Увеличение сопротивления повышает стабильность генератора и срок службы батареи, но приводит к снижению выходной мощности. Диаметр намотки контурной катушки — 5 мм, провод 0.5 мм.

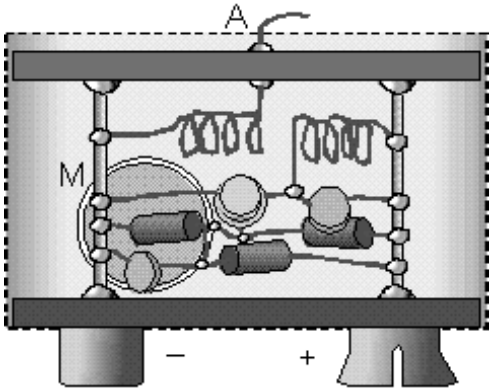
Число витков катушки для диапазона FM 5–6. Грубо рабочую частоту устанавливают подстроечным конденсатором контура, а точно — растяжением/сжатием витков катушки. Подстроечный конденсатор желательно заменить постоянным нужной емкости. Катушка связи расположена рядом с «горячей» стороной контурной катушки соосно на расстоянии 2 мм и содержит 4 витка того же провода.

Сближение катушек (вплоть до намотки катушки связи поверх контурной) и увеличение количества витков катушки связи увеличивает полезную мощность в антенне, но снижает стабильность частоты из-за влияния емкости антенны на настройку контура (т.к. каскад усиления мощности отсутствует). Поэтому ограничьтесь максимально возможной глубиной связи, при которой влияние расположения антенны в прост-

ранстве и касание ее руками не приводит к заметному уходу частоты передатчика.

Пример конструктива радиомикрофона

Этот радиомикрофон рассчитан на питание от батареи типа КРОНА и смонтирован на колодке от старой батареи.



С обратной стороны колодки впаиваются два штыря из луженой проволоки диаметром около 1 мм, и на них навесным способом распаивают детали. На выводах деталей пинцетом сгибают кольца и одевают на штыри. Такой монтаж обладает повышенной надежностью.

После регулировки схемы штыри обрезают на нужную длину и припаивают верхнюю пластину, которую можно сделать из обрезка старой печатной платы. На ней распаивают также вывод антенны. По завершении монтажа можно залить все эпоксидным компаундом и поместить радиомикрофон в металлический кожух (тоже берется от старой батареи). Напротив микрофона сверлят отверстие 2–3 мм.

Следует учесть, что заливка компаундом и наличие экрана могут повлиять на частоту настройки передатчика, так как диэлектрическая проводимость компаунда больше чем воздуха, и собственная емкость катушки увеличится (снижение частоты). Немагнитный экран приводит к некоторому увеличению частоты настройки. Для уменьшения влияния экрана располагайте катушку контура дальше от его стенок.

Слово о приемниках

Для приема радиомикрофонов замечательно подходят обычные радиовещательные приемники. Микрофоны диапазона 27 МГц лучше настроить немного ниже (24...26 МГц), чтобы их прием можно было вести на вещательный КВ приемник. УКВ микрофоны настраивают на свободный от вещания канал.

Достоинством применения вещательных диапазонов является то, что не требуется специальной аппаратуры, и можно использовать приемник магнитолы и вести одновременно запись на кассету.

Недостатки — вероятность того, что передачу может прослушать также и постороннее лицо, и низкая чувствительность/избирательность бытовых приемников, что в условиях городских помех сокращает эффективную дальность приема.

На радиорынках продаются модули для ремонта, представляющие из себя готовые приемники, усилители и т.п. Они отличаются малыми габаритами и невысокой ценой. С некоторыми доработками их можно использовать для создания специального приемника. Следует приобрести моно УКВ приемник на верхний диапазон (88–108 МГц) с одной контурной катушкой (такие приемники имеют низкую ПЧ и активные интегральные узкополосные фильтры). Такой приемник легко перенастроить за вещательный диапазон, только заменив контурную катушку. Достаточно удалить/добавить 1–2 витка. Невысокую чувствительность подобных приемников (обычно около 20 мкВ) можно довести до 2–5 мкВ, собрав входной усилитель. Лучшие результаты получаются с усилителем на полевом транзисторе с изолирующим затвором (типа КП350, КП306). За основу возьмите схему входного каскада промышленного тюнера. Входной контур (если он есть) также следует подогнать по частоте за вещательный диапазон.

Усилитель НЧ можно сделать самому. Желательно оснастить конструкцию выходом на наушники и для записи на магнитофон.

Настройка радиопередатчиков

Предварительную настройку передатчика производят на деревянном столе, с которого удалены все металлические предметы. При этом все сердечники вывинчивают из ВЧ катушек и подключают вместо микрофона НЧ генератор. Подают питание несколько ниже рабочего.

Для настройки очень полезен простейший волномер, состоящий из колебательного контура, параметры которого зависят от рабочего ди-

апазона. К нему подключается детекторный ВЧ диод, нагруженный на конденсатор 10 nF и микроамперметр на 50 uA (подойдет стрелочный индикатор уровня записи от кассетника). От трети витков контура делают отводок и к нему через конденсатор в несколько pF подсоединяют отрезок провода, служащий антенной. Волномер настраивают в резонанс по генератору ВЧ или «на глазок», по имеющемуся передатчику. Более крутой вариант имеет операционный усилитель после детектора, повышающий его чувствительность, и градуированную шкалу (обычно набор сменных контуров на разные диапазоны). Если вы планируете много возиться с жучками, лучше потрудиться и смастерить такой волномер. Для разовых целей подойдет и простейший.

Убеждаются в работоспособности генератора ВЧ с помощью волномера, поднося его антенну к контуру генератора. Если жучок работает в вещательном диапазоне, пытаются настроиться на волну с помощью приемника. Добиваются устойчивой генерации при сниженном напряжении питания и надежного запуска генератора. Плавно увеличивая напряжение питания, проверяют уход частоты от напряжения. При этом, если приемник позволяет, надо отключить в нем автоподстройку частоты. Слишком большой уход частоты связан с малой емкостью конденсатора обратной связи, включенным в цепи КЭ транзистора, так, что, собственная емкость транзистора, «плывущая» от изменения тока коллектора, сильно влияет на частоту настройки контура. Соответственно, исправляют увеличением емкости обратной связи и увеличением сопротивления в цепи эмиттера. Важно не переборщить, чтобы не возникало самовозбуждения генератора. Его признаками является «многочастотный» прием, посторонние шипы и свисты по диапазону. Помогает избежать — использование других деталей, укорочение их выводов до минимальной длины, другое расположение элементов монтажа.

Когда достигнута устойчивая генерация, к генератору подносят контур волномера и настраивают его на рабочую частоту. Затем подают полное напряжение питания, и, если есть, настраивают остальные усилительные каскады, пользуясь волномером как индикатором, и постепенно удаляя его от передатчика. Мощные выходные каскады нельзя включать без нагрузки, поэтому на время настройки вместо антенны подключают резистор сопротивлением 50...75 Ом. Окончательно настройку проводят, поместив волномер на расстоянии не менее 5 м от передатчика, подключив антенну, настраивая цепи ее согласования, а также подбирают длину антенны, откусывая от нее каждый раз по 1–2 см, или вращая сердечник удлинительной катушки. Затем снова проводят подстройку оконечного каскада.

В последнюю очередь настраивают звуковой тракт, добиваясь необходимой чувствительности и отсутствия искажений звука.

Часть 5. Тонкости, хитрости и секреты

Стандарты сотовой связи

В общем виде все стандарты можно разделить на аналоговые и цифровые. Аналоговые принято считать стандартами первого поколения, цифровые — второго. У каждого стандарта, кроме буквенного обозначения имеется еще и цифровое (например GSM-900, GSM-1800, GSM-1900). Цифра в названии стандарта обозначает рабочую частоту (GSM-900 работает на частоте 900 МГц (хотя, если говорить более грамотно, то в частотном диапазоне 890–960 МГц). Иногда, к примеру GSM-1800 называют модификацией стандарта GSM-900, а GSM-1900 — модификацией GSM-1800. Это действительно так, но в результате этой «модификации» возможности столь существенно изменяются, что гораздо правильнее называть их разными стандартами, созданными на основе более ранних версий. Еще одна очень важная вещь: рабочая частота определяет «дальнобойность» стандарта (чем меньше, тем дальнобойней), но в тоже время, чем меньше частота, тем меньшее количество абонентов может «сидеть» на одной «соте» (базовой станции).

Стандартный пример этому — Москва: в пределах столицы МТС и БИЛАЙН-GSM ставили станции GSM-1800 (большая плотность абонентов), а в Московской области — GSM-900 («дальнобойность» для покрытия большей территории) (для нормальной работы в таких условиях нужна трубка, работающая в двух стандартах, благо таких трубок предостаточно). Также используемый стандарт откладывает отпечаток и на мощность трубки — меньше «дальнобойность» — меньше мощность, дольше служат батареи, излучение трубки меньше бьет по голове...

Аналоговые стандарты

NMT-450/900

В России NMT-450 используется союзом операторов «Сотел». Стандарт является абсолютным чемпионом по «дальнобойности». Аналоговый звук в большинстве случаев гораздо лучше цифрового (имеется

в виду случаи, когда абонент удален от «соты» на некоторое расстояние, или находится в зоне сильных помех). Минусом стандарта является «привязанность» трубки к оператору, что фактически означает невозможность перехода в другую компанию (как правило Оператор NTM-450 в городе только один). Ну и большая мощность трубки конечно...

NMT-900 в России не применяется, его использовали только в Скандинавии, которая кстати и является родиной стандартов NMT (Nordic Mobile Telephone).

AMPS

Данный аналоговый стандарт впервые появился в США на два года позже, чем NMT-450. Advanced Mobile Phone Service, а именно так расшифровывается название данного стандарта, был довольно распространен в России на заре «мобильной эры» (в середине 90-х). Работает в диапазоне 824–894 МГц. Особых примет нет; можно сказать, что если NMT-450 еще держится, то AMPS уже точно — «вчерашний день».

Цифровые стандарты

GSM-450/900/1800/1900

Стандарты GSM на сегодняшний день являются самыми распространенными в мире (особенно в Европе). По статистике, доля стандартов GSM в Европе более 80%, в мире ~43%. Т.е. как ты видишь стандарты GSM можно смело назвать европейскими стандартами. Но не все виды GSM распространены одинаково: например GSM-450 в России вообще по-моему никто не видел, на GSM-900/1800 — работает примерно половина российских операторов, а вот GSM-1900 (его еще называют «американским GSM») можно в живую пощупать пока только в особо развитых странах...

Почему же он так распространен? Скажу честно — только потому, что трубки стандарта GSM являются абсолютно «независимыми» от Оператора (а также клонируются гораздо проще других современных стандартов). Ведь чтобы перейти к другому оператору нужно заменить лишь малюсенькую sim-карту, сделать это не просто, а очень просто, да и саму sim-карту другого Оператора можно купить буквально в любом ларьке/магазине — по-моему именно это люди и ценят. Ну и конечно же роуминг — такая высокая распространенность стандарта делает его довольно легким делом (да и можно устроить «сам себе роуминг» — достаточно просто купить в стране пребывания sim-карту местного оператора: номер телефона конечно измениться, зато выйдет существенно дешевле).

D-AMPS-800/1900

Цифровая вариация AMPS, широко распространенная в России. Из плюсов можно выделить довольно довольно большую зону покрытия (для D-AMPS-800, D-AMPS-1900 — чистый «американец», который в России не используется).

TDMA

Если у европейцев — GSM, то у американцев — TDMA, D-AMPS и CDMA. Многие считают, что TDMA превосходит аналогичный GSM-900. И это действительно не без оснований: в экстремальных условиях абоненты GSM нередко начинают «заикаться», а вот TDMA трещит, шипит, но держит голос таким, каким он есть...

CDMA-800/1900

Разработка американской фирмы Qualcomm, самый прогрессивный стандарт на сегодняшний момент. Знаменит высоким качеством звука, мощной защитой от двойников, низкой мощностью трубок. Единственная беда в том, что в России этот стандарт узаконен исключительно как «стационарный», т.е. телефон может находится только по определенному адресу, в связи с чем абсолютно легально подключают большие стационарные аппараты (похож на обычный, только с антенной сзади), трубки же идут «задним числом», поэтому не до конца законны.

Единственный минус — плохой звук во время движения, но при нынешнем уровне цен Операторов CDMA (от 0 копеек до 1–2 рублей за минуту) это конечно можно перетерпеть...

Как взломать автоответчик

Если ты не совсем уверен в том, что твоя подружка тебе верна, то для этого не нужно стоять под ее дверью с топором, яростно оберегая вашу любовь. Я, конечно, понимаю, что Варкрафт хоть уже и устарел, но все еще течет в твоих жилах, и порубать на винегрет любого придурка, вторгающегося в твою личную жизнь — давняя мечта. Но... Братишка, погоди пускать пар из ушей, может быть, твоя подруга и не виновата. В любом случае твоим подозрениям нужны явные доказательства. Иначе ты будешь выглядеть полным дураком, и в следующий раз она будет отмазываться, заявляя тебе, что ты слишком ревнив и ревнуешь безо всякого повода.

Итак, начнем нашу шпионскую деятельность с телефонии. Для начала проверим ее автоответчик. Дело в том, что большинство наших людей как были, так и остались «совками». И к импортной технике они

относятся как к хитроумным предметам, изучая только основные функции. У меня есть приятель в магазине, торгующем техникой, и вот он мне рассказывал, как у них новый русский покупал компьютер. Купил, отвез домой, а на следующий день приехал и говорит: «Ни хрена не понимаю. Как с ним обращаться-то? Есть какая-нибудь инструкция?». Мой друг ему отвечает: «Вам книжку нужно купить. Что-нибудь типа «PC для чайников»». Тот как закипит: «Ты кого чайником назвал? Ты че, в натуре! Не надо мне никаких книжек! Книжки пусть Пушкин читает. Ты мне объясни, на какую пимпу давить!» Вот так-то, приятель. Но вернемся к нашим баранам.

Итак, если у твоей подружки телефон с автоответчиком, то велика вероятность, что ты его сможешь взломать. У всех автоответчиков есть дистанционное управление с другого телефона. Для этого нужно только позвонить на автоответчик, перейти в тональный режим, и как только закончится приветствие, ввести код доступа, после этого автоответчик прокрутит в трубку все записанные сообщения. Круто? Вот этим-то мы и воспользуемся. Если родители твоей подруги не особо утруждали себя чтением инструкции и не устанавливали свой код доступа, то считай, что ты уже победил.

У всех автоответчиков есть «вшитый», фабричный код, который стоит по умолчанию. Если хозяин автоответчика код не менял, то установлен именно этот, фабричный код. Теперь тебе нужно узнать, какой тип автоответчика ты собираешься ломать. Это проще пареной репы. Сыграй на гордости его хозяина. Позвони своей подруге, и когда она поднимет трубку, скажи: «Привет, Марфуша. Я тебе сегодня уже звонил днем, автоответчик сработал, но пошла какая-то хрень, и он меня не захотел записывать. Что это у тебя за машинка-то? Советская, что ли?» Будь уверен, в ответ ты услышишь что-то типа: «Да ты что, офигел? Да у меня Панасоник! Последняя модель!» Что нам и было нужно. Теперь осталось только узнать модель, и можно начинать хакать. Продолжаем разговор: «Панасоник? А модель какая? Древняя какая-то, небось, раз так глючит». И тебе в негодовании скажут, какая модель, а если не скажут, то ты подскажешь, что номер модели всегда написан сзади.

Отлично, вся информация у тебя есть, теперь переводим взгляд на табличку, в которой долгожданные коды доступа.

Модель автоответчика	Код по умолчанию	Примечание
Panasonic 1000	369	Кассетный автоответчик-приставка. Код написан на нижней крышке и не меняется!
General Electric	Хххххх	Шестизначный код, написанный на нижней крышке. Забудь об этом.
Panasonic TM80/TM81	888	Цифровой автоответчик-приставка. Код вшит в память.
Panasonic 2395	X	Телефон с автоответчиком. Код написан на нижней крышке и состоит из ОДНОЙ цифры!!! (Создатель этой модели - наш человек) Тебе нужно максимум 10 раз на него позвонить.
Panasonic 2721 и 2470	111	Телефоны с двумя кассетными автоответчиками. Код вшит в память.
Все радиотелефоны Panasonic с частотой 46-49 MHz - с автоответчиками.	00 или 99	Радиотелефоны от Panasonic бывают 2-х типов: 46-49 MHz и 900 MHz. Здесь придется повозиться, чтобы узнать, в какой из них ты собираешься вероломно вломиться. Но я надеюсь, ты найдешь подход к "клиенту", и он тебе это расскажет.
LG (бывший Gold Star)	1111	Четырехзначный код вшит в память. Инструкция даже на русском настолько коряво написана, что, скорее всего, код не меняли.

Ну, конечно, конечно, я не стал сюда вписывать все существующие модели. Но я тебе кое-что подскажу. Если тебе назвали какую-то модель, которой нет в этой таблице — не отчаивайся. Беги в ближайший магазин, торгующий телефонами, найди там эту модель и попроси почитать инструкцию. Про код обычно пишут в рубрике «Setting remote code». Там будет всякая пурга, как его установить, а мелкими буквами написано, какой код стоит по умолчанию.

Грузим мобилу

Все это началось с того, что меня достал один придурок с мобилой!

А так как никто не любит чтоб его доставали... я начал искать способы как ему отомстить и после долгих раздумий решил отыграться на его телефоне!

Всем известно, что многие сотовые операторы выделяют email на номер: xxxxx@host_operatora. Вот я и решил сначала подписать этот номер на кучу бесплатных рассылок, но этого мне показалось мало, к тому же там часто подтверждение требуют. После еще некоторых раздумий меня осенило!

Я зашел на http://www.rambler.ru/, открыл два бесплатных e-mail и в настройках установил следующие фишки:

1. Уведомление о получении письма отправляем на xxxxx@host_operatora, благо rambler не требует подтверждения от жертвы как это делает chat.ru.

2. Письмо пересылается в другой ящик.

3. Потом удаляется.

Потом просто отправляешь с одного мыла на другое. И оно зацикливается. Вот и все. Так же можно вместо xxxxx@host_operatora написать любой e-mail и mr.Rambler сделает сам всю черную работу.

Может кто и скажет, что прикол голимый, но он работает, и работает очень офигенно. У моей жертвы телефон звенел каждые 5 секунд! — прикольно, не так ли??

Как «хакнуть» абонента сотовой сети МТС

Короче, тебе потребуется:

1. Твоя голова.

2. Сотовый телефон (твой и желательно Nokia или Siemens).

3. Сотовый телефон (друга ломака).

4. Компьютер с доступом в Интернет (твой или в Интернет кафе).

Для начала хочу сказать, что это не является хакингом вообще, это лишь показывает, какие в нашей стране доверчивые люди и какая тупая система Интернет сервиса абонента у компании МТС (сравнить даже с системой Билайн).

Как ты наверно уже знаешь, у компании МТС есть Интернет система сервиса абонента (ИССА). При покупке телефона у абонента эта система отключена «по умолчанию».

Нам надо сделать так чтобы эта система включилась, а делается это так.

Берем у своего недруга телефон, буквально на одну минуту под любым предлогом и набираем следующий номер: 08802445 т.е. включаем ИССА, после того как мы ее включили нам надо установить пароль для доступа в ИССА, для этого мы звоним по номеру: 088021 и устанавливаем пароль (пароль не должен быть больше 7 цифр), по окончании ввода пароля нажимаем звездочку и обрываем вызов.

Теперь ты можешь смело входить на сайт компании www.mts.ru под реквизитами ламака и творить с его телефоном все что угодно, например узнать сколько денег осталось у него на счету, добавлять ему дополнительные услуги, отсылать себе за его счет логотипы, мелодии и т.д., вплоть до добровольной блокировки его телефона на какой угодно срок.

Скрытие своего телефонного номера

А вам когда-нибудь приходилось любоваться матрицей... В смысле вы не думали, что при надобности, ваш звонок по телефону всегда можно отследить... О чем я?

Простенький пример: один человек, назовем его X, решил разыграть одну бабушку, разыграл... А бабуля после его звонка пошла к своей бабушке-подружке, позвонила на телефонный узел и попросила сказать ей номер, с которого производился последний звонок (в ядре матрицы хранится номер последнего звонка, хотя на новых цифровых АТС на каждого юзера телефонной сети уже имеется лог на все звонки). Все, X, был найден и...

Или другой пример: вы решили позвонить провайдеру одного ламака, логин/пароль которого неожиданно оказался у вас по велению старика Билла Хоттабыча, провайдер имел АОН. Все, вам хана... Агент Смит через пару часов будет у вас на своем черном джипе и в компании 4–5 мускулистых дяденек, которые снимут с вас долларов 400 или просто банально сломают вам ноги (в случае одного из московских провайдеров на букву «М» именно так обычно и бывало).

Меры противодействия

Один мой кореш в свое время юзал этот самый «халявный и-нет» от провайдера М. После первого звонка от прова, в котором злой админ матерился и требовал прекратить акты вандализма по отношению к М., он пришел ко мне. Подумав с минуту, я предложил подключиться к телефонному кабелю, который проходил в его щитке. Так и сделали, был собран тоновый генератор, который давал гудок в трубку несчастных, чей телефонный номер мы использовали (чтобы не догадались, если вдруг решат ночью снять трубку; правда на попытки набрать номер гудок не откликался и продолжал гудеть), ну и начал мой кореш юзать халяву...

Кстати хочу отметить, что мы отрубали на ночь соседский телефон и подключали к нему тоновый генератор, а в это время использовали инет, а с утра все возвращали как было. Итак, через 3 месяца вдруг мой кореш увидел 2 джипа и не скольких «маленьких» дяденек, которые зашли в его подъезд... по счастью они пошли выше его квартиры, в ту самую, к телефону которой мы подрубились. В ней жили старички — дед с бабкой, представляете сколько было эмоций, когда дяденьки обвинили их в по-

стоянном хакерстве и потребовали предъявить компьютер, с которого оно производилось. Дальнейшая история мне не известна.

Другой мой знакомый написал программу, которая забивала его настоящий телефонный номер. Вкратце теория выглядит так: когда АОН (вам слышен при этом щелчок) берет трубку, он посылает запрос АТС, которая передает в ответ на него номер звонящего. Обычный анти-АОН работает так: он пытается не дать удаленному АОНу «услышать» ваш настоящий телефонный номер. Его же программа передавала ложный номер (обычно 666-6666 [Москва]), правда иногда удаленные АОНы «смешивали услышанное» и получалось что-то вроде (987-0769). Однако в ядре матрицы все равно обычно оставался его настоящий номер.

Как я вам показал, способы скрыться от матрицы есть, но они весьма ненадежны! Поскольку сейчас есть специальные приборы (используют работники АТС), которые с точностью до метра скажут работнику АТС, где произведено несанкционированное подключение к номеру... Скрыть свой настоящий номер программными методами со 100% вероятностью то же нельзя...

Решение

Долго в воздухе витала идея, которую оформил в слова уважаемый мною LovinGod (http://lovingod.cjb.net). Вы наверняка видели телефонные карты международной/междугородней телефонии. Ну так вот, смысл таков: вы звоните на телефонный номер телефонного оператора, переходите в тональный режим и вводите пин-код с карты, а затем номер, можно в Москве (Питере, или в Америке). Ну так вот... Но номер определится не ваш, а номер ПУЛА ОПЕРАТОРА в данном городе/стране. Но ведь можно выстроить цепочку из таких операторов и через 10 городов, а то и стран... Таким образом, отследить вас смогут только очень могучие силы. Как вы понимаете, таким образом вы, хотя и заплатив за карты, практически блокируете возможность вашего обнаружения.

Окончательное решение

Если вы хотите на 99,9% процентов обезопасить себя рекомендую делать так: через сеть купить несколько карт (около 10) и использовать чередование обычных и карт IP-телефонии. Рекомендую так же использовать подключение к чужому номеру телефона, тогда искать незаконное подключение, даже в самом плачевном случае, если цепочку отследят, будет поздно, т.к. вы уже отключитесь. Самое уязвимое место в этом мероприятии — покупка карт. А для стандартных целей (если вы не решили бороться со всем миром сразу) достаточно и одной карты. К примеру, звоните из Москвы в Питер на номер пула своего же провайдера телефо-

нии, вводите там реквизиты своей же карты и звоните обратно в Москву. Вот и все, ваш номер скрыт.

SMS-этикет. 10 очень важных правил для текстовых сообщений

Обмен текстовыми сообщениями одна из самых простых и распространенных форм общения в современной мобильной связи. Но иногда этот сервис доставляет пользователям некоторые неудобства. Чаще всего это происходит потому что владельцы карманных компьютеров и сотовых телефонов не учитывают особенности 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 10 общих правил мобильной переписки для всех государств. Итак:

1. Обрывать SMS-беседу без объяснения причины так же грубо, как и неожиданно положить телефонную трубку в самый разгар разговора.

2. SMS — средство неформального общения. SMS не должны использоваться для официальных приглашений или информирования о важных известиях.

3. 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.

4. 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.

5. Не следует пользоваться SMS, занимаясь другими делами. Это запросто может обидеть адресата письма.

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

7. Не стоит забывать, что координаты отправителя SMS можно легко вычислить. Анонимные сообщения лучше посылать с Интернет-сайтов.

8. Не надо донимать SMS-беседами по ночам. В то время как одни люди поздним вечером могут бодрствовать, другие уже давным-давно спят.

9. 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.

10. Всегда стоит помнить, что мобильный телефон в любое время можно выключить. На свете есть много вещей, которые, на самом деле, могут подождать.

Разлоченные телефоны могут вредить абоненту

В большинстве европейских стран существует возможность купить мобильный телефон за символическую сумму. Низкая цена обусловлена тем, что такой телефон работает только с подключением к определенному оператору связи. Для того, чтобы «залоченный» телефон работал через любого оператора, необходимо произвести его «разлочку». Это осуществляется заменой прошивки телефона (firmware). Как правило, такие телефоны легально не продаются. Это так называемые «серые» телефоны. Рынок подобной техники достаточно велик. Как утверждают некоторые источники, приблизительно 15–18% пользователей последние 6 месяцев используют такие телефоны (что наносит фирмам, производящим трубки, ущерб более 1,5 млн. евро). Кроме того, что «разлочка» телефонов незаконна, существует ряд проблем, связанных с безопасностью. Многие современные телефоны используют ОС Symbian и подвержены заражению вирусами. Известен ряд случаев, когда приобретенные на «сером» рынке «разлоченные» телефоны были заражены Cabir и другими malware. Другая опасность содержится в самой новой прошивке. Она может содержать код, который будет использовать какой-нибудь незаказанный сервис, и оплата его может обойтись для пользователя в сумму до нескольких сотен евро. Средства массовой информации сообщают, что в Европе уже зафиксированы подобные случаи, проводятся расследования.

Фрикинг контроллера транковой платы

Для того, чтобы зайти в контроллер по служебному паролю, нужно знать номер телефона, к которому он подключен. Модем может быть любым. Необходимо набрать номер телефона следующей командой:

```
ATDP1234567 r
```

Либо с параллельного телефона набрать номер, а после ответа модема на контроллере набрать в терминале АТА и нажать **Enter**.

Пробелов между номером и командой «**r**» может быть от 1 до 3. В зависимости от количества пробелов изменяется время ожидания. После снятия модемом контроллера трубки, ваш модем начинает устанавливать связь. Далее вы видите на экране сообщение:

```
CONNECT1200/NONE
```

Необходимо ввести один из служебных паролей:

```
0(пробел)(пробел)0
```

или

```
5(*)0(пробел)
```

(Скобки вводить не надо).

Далее действуете в соответствии с описанием на контроллер ST-852.

Один из паролей работает на старой версии контроллера, другой — на новой. Но хочется отметить, что способ связи с помощью команды ATDP... не блещет удобствами. Связь устанавливается не всегда, так как модем начинает устанавливать связь то раньше, то позже, и поэтому рекомендуется набирать номер вручную, предварительно открыв терминальную программу и набрав АТА, и после снятия удаленным модемом трубки нажимать клавишу **Enter**, завершая ввод команды.

Нечего и говорить, что эти пароли работают и при связи через Com-порт!

В случае, если вам попала в руки транк-плата и вы мечтаете использовать ее у себя в радиостанции или хотите посмотреть ее содержимое!

Например, Motorola GP-68. Бывают «тупые» провайдеры, которые при забытии ими же поставленного пароля, просто выбрасывают транк-плату. *Глупо.* Достаем Транк Плату (ТП) из радиостанции и ищем чип, у которого восемь ног, это и есть последовательная флэш память, в которой хранятся все настройки ТП (пароль, код абонента, количество сканируемых каналов). В случае, если вам надо знать, что внутри ее записано, то придется ее выпаять и прочитать на программаторе или любым

процессором по протоколу, описанному специально для этой памяти. В данной плате установлена память фирмы ISSI IS93C56-3. Скачать описание этой микросхемы можно по адресу www.issi.com или поискать через www.altavista.digital.com «is93c56-3».

Вам будет несложно разобраться, где и что находится в памяти, там ничего не закодировано и читается прекрасно, только «задом наперед».

Например, пароль выглядит **05 04 03 02 01**. Как известно, пароль по умолчанию **12345**. Необходимо заметить, что системные параметры читаются из памяти в процессор только при включении питания станции.

Если вам наплевать, что внутри памяти, то вперед! Ставим ТП на место, припаиваем провод на корпус, а второй конец, на 6 ногу микросхемы памяти и... включаем питание, откусываем провод, выключаем, включаем Р/С и... транк-плата девственно чистая, то есть по умолчанию.

Это происходит потому, что процессор не может получить выходные данные от микросхемы памяти (так как мы закоротили DOUT) и сам зашивает в нее все параметры по умолчанию. Войти в режим программирования ТП можно удержанием кнопки «решетка» и одновременным включением питания, далее 12345 и опять «решетка», высокий тон значит вход, а низкий тон... (наверное, корявые руки или длинные ногти).

Можно поставить в транк-плату процессор, который будет сканировать из эфира пэйдж-коды и подсовывать процессору ТП. И тогда звоните сколько влезет, выследить вас тяжело.

Фрикинг телефонных карточек

Чип, который стоит в телефонных карточках, зависит от производителя карточки. Во французских карточках, которые еще продаются в Москве, стоит чип ST1331 фирмы SGS-Thomson.

Телефонную карточку восстановить нельзя. Карта устроена таким образом, что деньги на ней можно только уменьшать. Для этого обычно используется восьмеричный счетчик на EEPROM с хитрой логикой управления, позволяющей записывать в счетчик только значения, которые меньше текущего значения счетчика.

Эмулятор карточки — это устройство, собранное на микроконтроллере, эмулирующее работу телефонной карточки. Эмулятор можно сделать для любой телефонной карты.

Фальшивый номер звонящего абонента

Когда-то это была веселая шутка — подделывать номер какой-нибудь радиостанции и звонить людям — раздавать подарки. Это сделать не сложно. Ваша задача: позвонить с телефона, с которого не определяется номер и послать в нужный момент сигнал «ответ АОН». Этот сигнал содержит номер и категорию абонента. Этот сигнал длиной 360 мс постоянно повторяется 2–4 раза при стандартном определении номера на АТС. Вам лучше прокручивать его секунды две.

Таким образом:

- открывается wav файл с сигналом в звуковом редакторе или плейере;
- ставится режим **loop** для того, чтобы данный сигнал постоянно повторялся;
- прикладывается к телефонной трубке (к микрофону) колонка саундбластера;
- ставится нормальный уровень громкости (немного выше среднего);
- звонится человеку, у которого АОН, с телефона, номер которого не определяется. Как только на том конце поднимут трубку — АОН начнет пипикать (это запросы на выдачу сигнала «ответ АОН»);
- как только будут услышаны эти запросы, нажимается пуск.

Через пару секунд можете выключать.

Номер подделан — можете пудрить мозги вашему собеседнику.

Сигнал можно сгенерировать с помощью специальной программы **Blue box generator** или в программе **Sound Forge: Tools\Synthesis\DTMF,MF**. Тип сигнала MF, длина 0.040, пауза и break 0.001, от **Fade in the edges** «птичку» убрать, в строке **Dial string** записать **1xxxxxxx***, где **xxxxxxx** — это семизначный номер, записанный задом наперед!!! В случае, если количество цифр номера меньше семи, дополните его кодом города. Просмотрите всю комбинацию справа налево, если заметите, что цифра повторяется (левая цифра повторяет правую), то замените повторяющуюся (левую) цифру на символ «B», так как не должно быть рядом стоящих цифр. И не забудьте про звездочку в конце.

Например,

```
номер (8-09612)56789 = 19876521*;номер (8-095)3881299 = 1B921B83*
```

Russian GrayBox

Russian GrayBox — устройство для подмены номера по запросу АО междугородней АТС. На некоторых типах АТС возможно создать ситуацию, когда запрос АОН междугородней АТС попадает непосредственно на ваш абонентский комплект, а не блокируется станционной аппаратурой. Russian GrayBox эмулирует ответ вашей АТС и посылает ложный безынтервальный пакет с чужим номером. В этом случае АТС считает, что звонок по межгороду идет с другого номера (который подставлен в безынтервальном пакете) и счет за переговоры приходит на другой номер.

Russian GrayBox работает только на старых типах АТС. Найти их в крупных городах практически невозможно. Устройство Russian GrayBox существует как в переносимом, так и в упрощенном портативном варианте в виде бипера.

«Кульный девайс»

Кульный девайс — это фрикерский комплекс, позволяющий вести эксперименты с системой телефонной сигнализации на территории бывшего СССР. С помощью него можно, к примеру, позвонить по межгороду по очень низкой цене. Или попробовать подсоединиться к занятой линии. Сделать «кульный девайс» очень просто: надо взять любой модем, умеющий генерировать однотональные и двухтональные сигналы произвольной частоты, амплитуды и длительности в линию. Такими модемами являются, к примеру, модифицированный USR Sportster (Russian Courier), модифицированный USR Courier или Digicomm Connection 14.4+ и другие. Затем нужно написать соответствующую управляющую программу на компьютере.

Системы сигнализации

В основном, используются две системы, доступные для исследований: одночастотная и двухчастотная. Одночастотная система использует сигнал 2600 Hz и сигналы «2 из 6» для передачи контрольной информации и набора номера, двухчастотная система использует для этих целей различные комбинации частот 1200 и 1600 Hz. Система двухчастотной сигнализации является более старой и в настоящее время используется все реже. Определить тип сигнализации, используемой в междугороднем канале, можно на слух: если при соединении или разъединении слышен однотональный сигнал, то используется одночастотная система, если слышен характерный двухтональный сигнал — используется система 1200/1600.

Телефонные блокираторы

Блокиратор предназначен для подключения дополнительного телефона к любой телефонной линии наряду с основным телефоном, при этом за основным телефоном сохраняется полный приоритет, а именно:

- если на основном телефоне поднята трубка, то с дополнительного телефона позвонить и прослушать разговор на основном телефоне нельзя;
- если трубка основного телефона поднимается во время разговора на дополнительном, то разговор на дополнительном телефоне прерывается и он отключается от линии.

Блокиратор имеет индикаторный светодиод, который индицирует подключение основного телефона к линии. Его свечение означает, что поднята трубка основного телефона либо идет звонок вызова на основной телефон. Подключается: -60В линии к общему проводу блокиратора, в разрыв провода и +60В хозяина, затем +L к линии (входной) и TF0 к хозяину (выходной). Подключаться удобнее следующим образом:

- Тестером все промеряется и подключается со строгим соблюдением концов и полярности.
- Перерезается провод +60В между нашими двумя проводами. При отключенном питании линия подключена к хозяину.

Тянуть удобнее всего обычной телефонной «лапшой» в два провода (четыре жилы), при этом один целиком земляной (две жилы), а другой к плюсовому проводу линии в соответствии с описанным выше. Две телефонных лапшички и приколачивать к стене удобнее и меньше обращает внимания на себя. Скрутки засовываются глубоко в кабельный канал.

Фрикинг таксофонных карточек

Не так давно на российского потребителя обрушился целый поток новых платежных средств: таксофонные карты, магнитные карты метро, банковские карты. Коснемся пока только таксофонных карт. Наверное,

каждый задавался вопросом, как же устроена и как работает таксофонная карта, и можно ли ее обмануть. Ответ на второй вопрос пока умолчим, а вот на первый попробуем ответить в доступной и популярной форме. Разговор пойдет конкретно про таксофонные карты компании «Санкт-Петербургские таксофоны». Для других карт приведенная информация может не соответствовать действительности.

Таксофонная карта соответствует международному стандарту ISO 7816 в части 1 и 2.

```
ISO 8716-1:1987 Карточки идентификационные.
Карточки на интегральных схемах с контактами.
Часть 1. Физические характеристики.
СТК 1 код В 4 с. изд.1

ISO 8716-2:1988 Карточки идентификационные.
Карточки на интегральных схемах с контактами.
Часть 2. Размеры и расположение контактов.
СТК 1 код D 7 с. изд.1
```

Кристалл на карте представляет собой электрически программируемое ПЗУ с последовательным побитным выводом информации, изготовленное по технологии NMOS. В этом ПЗУ используется 128 бит. Для того, чтобы перепрограммировать карту, нужно стереть информацию из ПЗУ, но чип защищен от ультрафиолетового облучения специальной смолой. Даже если вам удастся стереть чип, то нужно будет перепрограммировать специальную область производителя — первые 64 бита, а она защищена от записи плавким предохранителем, который пережигается на фабрике при производстве чипа. Основной способ обмана таксофонов — изготовление эмуляторов, то есть устройств, эмулирующих работу настоящей карты. Это довольно легко сделать на современных однокристальных микроЭВМ. Основной способ защиты таксофонов от таких эмуляторов — измерение межэлектродных сопротивлений, емкостей и сравнение их с номинальными, что позволяет таксофону отличить эмулятор от настоящей карты.

Чтение информации с карты

Внутри карточки находится счетчик адреса разрядностью 9 бит. То есть после чтения каждых 512 бит все начинается сначала. Счетчик может быть только увеличен. В случае, если вы хотите считать бит с адресом меньше текущего, то счетчик нужно сбросить в 0, а затем увеличить до необходимого значения. Операция сброса выглядит так: надо установить высокий уровень сигнала Reset (2 контакт карты), а затем установить и сбросить сигнал Clk. После сброса сигнала Reset на выходе (7 контакт карты) будет доступен бит с адресом 0.

Теперь нужно подавать тактовые импульсы на вход Clk (3 контакт карты). По фронту импульса происходит увеличение на единицу внутреннего счетчика адреса.

По спаду тактового импульса следующий бит данных появляется на выходе. Обычно удобнее представлять информацию в виде байтов. Для этого каждые 8 считанных бит группируют в байт, считая, что первым считывается наименее значащий бит.

В итоге, последовательно считывая 1,0,0,1,0,1,1,1, получим байт 0xE9.

Чтение через параллельный порт компьютера

Поскольку все сигналы соответствуют уровню ТТЛ, то логично использовать для чтения информации обыкновенный принтерный порт. Не думаю, что надо приводить здесь полное техническое описание работы параллельного порта, назначение контактов и описание портов ввода-вывода — это все можно найти в специальной технической литературе.

Аппаратные средства

Аппаратные средства представляют собой ответную часть разъема параллельного порта, кусок монтажного провода и считывающее устройство, которое может представлять собой обыкновенный кусок текстолита с отверстиями, в которые вставлены штырьки. Правда, в этом случае карточку надо будет прижимать руками.

Программные средства

Используем порт LPT1. Запись в принтерный порт осуществляется через порт 0x378. Записанный байт появляется на выходных контактах. Мы используем бит 0 для сигнала Reset и бит 1 для сигнала Clk. Чтение выполняется через порт 0x379. В самом старшем бите появится инвертированное значение с входного контакта 11 (Busy).

Что именно записано на карте

Теперь мы и подошли к самому интересному месту — назначению каждого бита, записанного на карте. Естественно, что на картах других городов это назначение будет другим, но мы, как обещали, говорим о питерских карточках. На карточке используются только 16 байт. Все остальные равны 0xFF. В процессе исследований было проанализировано около 300 карточек.

Примеры дампов памяти карт

- Эта карта на 50 единиц закончилась. Номер 0050415503. Годна до 30.09.2005

```
E9, 30, FF, 01, F1, E2, 80, C0
00, 00, 00, 00, 00, FF, 18, EA
```

- Эта карта на 400 единиц также пуста. Номер 0400155921. Годна до 30.09.2005

```
E9, 30, FF, 01, 88, A7, 9B, E8
00, 00, 00, 00, 00, FF, D9, 79
```

- Вот карта на 1000 единиц. Осталось 998. Номер 1000013039. Годна до 31.12.2006

```
E9, 30, FF, 01, F7, 3F, 59, DC
00, 01, 7F, 0F, 3F, FF, 68, 6B
```

- Потом я позвонил по этой карте. Осталось 6 единиц.

```
E9, 30, FF, 01, F7, 3F, 59, DC
00, 00, 00, 00, 3F, FF, 68, 6B
```

- Наконец, она закончилась.

```
E9, 30, FF, 01, F7, 3F, 59, DC
00, 00, 00, 00, 00, FF, 68, 6B
```

Назначение полей

- Первые 4 байта — какой-то идентификатор. На всех картах E9, 30, FF, 01.
- Следующие 4 байта — серийный номер карты. Расположив биты в байтах в обратном порядке, а затем и сами байты, получим 32 разрядное целое без знака. К примеру, байты F7, 3F, 59, DC с обратным порядком бит выглядят как EF, FC, 9A, 3B. Получим номер карты 0x3B9AFCEF или 1000013039 в десятичном виде. Нетрудно заметить, что номер, напечатанный на карте, всегда состоит из 10 цифр, а первые 4 цифры — емкость карточки.
- Следующие 5 байт — количество единиц, оставшихся на карточке. Формат хранения очень интересный: используется количество единичных битов в байте, начиная с младшего. Соответственно значение байта 07 соответствует 3 единицам, значение 1F — пяти, а 7F — семи единицам. Максимальное количество единиц, хранящихся в байте — семь. Соответственно используется

восьмеричная система счисления. В итоге, байты 00, 01, 7F, 0F, 3F соответствуют 01 746 в восьмеричной системе или 998 единиц в десятичной системе. Максимальное количество единиц может выражаться числом 77777 в восьмеричной или 32767 в десятичной системе.

- Следующий байт всегда равен FF. Похоже, он не используется.
- Два последних байта, по-видимому, выражают CRC или другой контрольный код для первых 8 постоянных байт, так как при расходовании единиц они не меняются, но на каждой карточке они свои. Пока их назначение не ясно.

Обнаружилось, что срок годности не записан на карте. По всей видимости, он как-то связан с номером карты. Возможно, каждому сроку годности соответствуют определенный диапазон номеров.

Как уже говорилось, из 10 цифр номера первые 4 выражают емкость карты. Оставшиеся 6 не идентифицируют карту однозначно, так как уже выпущено более миллиона карт. Всего при подобной системе нумерации может существовать 6 миллионов карт:

- На 25 единиц с номерами от 0025000000 до 0025999999
- На 50 единиц с номерами от 0050000000 до 0050999999
- На 100 единиц с номерами от 0100000000 до 0100999999
- На 200 единиц с номерами от 0200000000 до 0200999999
- На 400 единиц с номерами от 0400000000 до 0400999999
- На 1000 единиц с номерами от 1000000000 до 1000999999

Устройство для чтения/записи магнитных карточек

Для изготовления устройства, которое, разумеется, можно применять не только для чтения, но и записи магнитных карточек, удобно использовать готовый лентопротяжный механизм магнитофона или плейера. Карточка при этом протягивается так же как и лента, между тонвалом и тонроликом. Но надо иметь в виду — металлический тонвал проскальзывает по пластиковой поверхности телефонной карточки. Автор надел на тонвал тонкую ПВХ трубочку от изоляции импортного экранированного провода, предварительно окунув ее в ацетон. После высыхания ацетона можно включить моторчик ЛПМ и подшлифовать внешнюю поверхность трубки мелкой наждачкой. Подготовка приводного вала — очень

важный момент! Именно от вала в основном зависит равномерность скорости подачи карточки. Впрочем, остальные узлы тоже требуют аккуратности. Несмотря на это, устройство полностью можно изготовить за пару выходных дней.

После подготовки вала нужно изготовить направляющий тракт. Его конструкция зависит от конкретного ЛПМ. В качестве исходного материала можно использовать двухсторонний фольгированный стеклотекстолит. Его легко обрабатывать и соединять детали пайкой, без дополнительных крепежных деталей. В конструкции используется пара светодиод-фотодиод для регистрации моментов начала и окончания прохождения карточки через ЛПМ. Необходимо учитывать, что запись начинается примерно в 3 мм от края карточки и располагать головку так, чтобы тонвал успел захватить и начать протаскивать карточку до того, как начало записи окажется в рабочей зоне головки. Примерно в этот же момент должен срабатывать и оптодатчик. У меня карточка после прохождения ЛПМ по инерции проскакивает дальше и открывает оптодатчик снова. Но лучше поставить второй оптодатчик на окончание карточки, чуть правее оси магнитного зазора головки.

Особую сложность представляет только узел крепления головки, так как надо прижимать головку к карточке, а не наоборот. Площадка с прикрепленной к ней головкой равномерно прижимается четырьмя пружинками. Прижимное усилие должно быть небольшим, так как магнитный слой намагничен очень сильно. Сохранена возможность регулировки азимута головки. Провода, идущие от головки — тонкие неэкранированные, не должны мешать смещению площадки с головкой. Они подведены к контактным площадкам недалеко от головки. Далее идут экранированные провода. Моторчик питается непосредственно от 5-вольтового напряжения питания всей схемы. Моторчик от плейера обеспечивает при этом необходимую скорость движения карточки. Помехи легко шунтируются керамическим конденсатором, расположенным на выводах моторчика.

Фрикинг таксофонов

Способ первый

На старых автоматах иногда не работает, но на новых без проблем! Фокус заключается в том, что, после того как на том конце поднимут трубку, нужно резко дернуть рычаг сброса вниз, не забыв его отпустить. И пожалуйста говорите... В случае, если дернуть медленно может разъединить. В случае, если слишком быстро — не всегда соединяет. Просто передерните этот рычажок под трубкой. Работает безотказно!

Способ второй

Когда жетон торчит в монетоприемнике, створки закрыты. При поднятии трубки отвечающим створки отодвигаются или приподнимаются и опускаются, роняя ваше богатство вниз. С момента опускания створок вниз и до момента задевания летящим жетоном рычага внутри аппарата вы ничего не слышите. Так и будет, если жетон не заденет этот рычаг. В случае, если створки не смогли приподняться, то звук не исчезает, и вы можете свободно говорить. Используя ключ или спички, вы можете надавить на створки, и, пока не отпустите, можно разговаривать. Надавливать нужно в левую или правую часть щели — вы почувствуете, что они пружинят.

Способ третий

Единственный Жетон, который вам дорог, как память, как можно сильнее запихайте в щель телефона. Надавите на него посильнее (одновременно придерживая) и держите так. Створки не приподнимутся — звук не исчезнет.

Способ четвертый

Сделайте из плохо гнущейся проволоки подобие клюшки.

Опустите ее в правую часть щели загнутой частью направо и, при соединении, нащупайте ею рычажок внутри аппарата. Трахать до полного оргазма (телефон сообщит вам об этом сладострастными звуками включенных микрофона и динамика).

Способ использовался во Владивостоке для междугородных переговоров. Там же, возле автоматов, нас научили правильно им пользоваться, я даже видел у одного из звонящих клюшку с декоративной деревянной ручкой.

Способ пятый

Кусок провода. Один конец вставьте в микрофон, установив контакт с его поверхностью, другой — зажмите в железном шнуре трубки (земля). При полном контакте можно не ломать оборудование и не мучить ass автомату; спокойно при этом разговаривая. Током не стукнет.

Способ шестой

Видели ли вы автоматы с расширенной путем раздалбливания щелью монетоприемника? Это сделано не зря. Опущенная вместо жетона крупная монета застрянет в желудке у жетоноядной твари.

При нажатии на рычаг в животе у нее будет булькать, но акта дефекации в коробку с жетонами не произойдет. Наберите номер, дождитесь поднятия трубки. Теперь аккуратно рычагом (не сбросьте связь) подергайте так, чтобы звук появился. Он появится.

Модернизация телефонных карт

Как сделать вечную телефонную карту: нужно всего-то раздобыть телефонную карту, желательно пустую и не на помойке. Далее нужно взять фольгу (хоть от конфет «Мишка на сервере»). Я выдрал фольгу от сигарет. Фольгу нужно разрезать чуть больше, чем контактный чип. Еще нужно будет немного скотча. Скотч — это такая лента липкая, прилипает, где попало, и прозрачная. Разрезанную фольгу прикладываем на контактный чип и аккуратненько обклеиваем по краям скотчем. Вы заметили — по краям, не по центру, а по краям. Карточка готова к эксплуатации.

Ломаем АТС

Определение номера возможно только один раз, примерно в течение 0,3 секунды после соединения. АТС работает таким образом, что, когда абонент, которому звонишь, берет трубку, АТС в это время отключает тебя на десятые доли секунды, ну вот, как раз где-то на 0,3.

И после того, как АТС тебя отключила, если у того абонента стоит АОН, он начинает слать запросы (тональные посылки), их можно услышать в трубку, но если пауза перед определением получается слишком большая, то просто можно услышать щелчок, АТС начинает слать ответ, происходит определение номера, после чего пойдут длинные гудки, но посылаемые не АТС, а уже АОНом, определившим твой номер или заглючившим и не определившим твой номер. Некоторые АТС «все равно» шлют ответ, не обращая внимание, стоит там АОН или нет. Сам этот ответ не слышно, так как АТС тебя в это время отключает, а абонент, которому звонишь, его может прекрасно услышать в динамик АОНа, если там есть функция «прослушивание ответа АТС в режиме автоподнятия». В случае, если же нету, то его можно прекрасно услышать, если на АОНе стоит определение после поднятия трубки. Для того, чтобы звонить на «чей-нибудь» номер, нужно сначала заблокировать АТС, чтобы она не слала ответ. Для этого на АОНах есть функция Анти-АОН, или, если нету, то можно воспользоваться просто набором цифр, к примеру «0», так как «0» самый «большой».

И это надо делать не сразу! Это делается после того, как происходит соединение! Потому что на современных АОНах можно ставить до 99-ти запросов! И если нажать Анти-АОН сразу, то АТС на этот момент, пока работает Анти-АОН, отвечать не будет, но стоит только ему «закончиться», а АОН все еще будет слать запросы, то АТС сразу же ответит!

Можно сделать так, подержать подольше Анти-АОН, АОН закончит слать запросы, ну, номер не определится, собственно для чего Анти-АОН и нужен. Но если звонить по межгороду, АТС сделает несколько запросов, номер не определится, и тебя «выкинут».

Так вот, Анти-АОН включается сразу же после того, как только услышал запрос АОНа или щелчок. Удерживать около 0,5 сек, потом сразу нажать «#»! АОН будет продолжать слать запросы, но уже бесполезно. Однако если звонить по межгороду, то это не бесполезно! И в этот момент, пока АОН шлет запросы, нужно посылать свой ответ.

Что для этого нужно? Для этого нужен Sound Blaster, самый древний дисковый телефон (главное, чтобы трубка работала) и какой-нибудь *.WAV recoder. Вытаскиваешь из трубки два провода и вставляешь в MiC Blaster'а (рекомендую припаять к проводам штекер, а не совать так). Потом ставишь на АОНе определение после поднятия, берешь, просишь, чтобы тебе кто-нибудь позвонил. После того, как у тебя зазвонил телефон, включаешь **REC** в своем **.WAV** редакторе и поднимаешь трубку на любом телефоне, записываешь ответ от АТС, потом говоришь «спасибо» тому, кто тебе звонил, редактируешь **.WAV**, убираешь все лишнее.

И все Ok! Да, АТС отвечает не один раз, а от 2-х до 4-х. В принципе, это не мешает делу. Но когда будешь редактировать, будет очень неудобно, советую обрезать! После того, как отредактировал свой .WAV, перетыкиваешь штекер в Speaker, звонишь кому-нибудь еще (можно тому же), после того как АОН поднимает трубку, блокируешь определение и нажимаешь **PLAY** (засылаешь этот ответ). Я думаю, что своих корешей (или кого-то там еще) подставлять нехорошо. Для этого, берешь и извращаешься с WAV'ом... А лучше, берешь в recoder'е функцию «Reverse» и сам понимаешь. Кому придет идея в голову посмотреть номер наоборот?

Да, в телефоне не семь цифр, а восемь! Последняя означает категорию абонента, она почти у всех «1», так что номер в обратную сторону будет начинаться на цифру «1». «3» — это абонент без выхода на междугороднюю связь, не редактируй **.WAV** так, чтобы последняя цифра была «3»! Да, если эта 8-я цифра будет «4» или «7», то счет никому не придет!

На межгороде определение происходит после набора номера, а на некоторых, особенно на декадно-шаговых АТС, после выхода на межгород «8». Запрос можно и не услышать, можно услышать просто щелчок.

Но там нужно быстрее слать ответ! Там такая хитрая система, что, если номер не определится, даже если вы сделаете все как надо, АТС сделает еще запрос и номер все равно определится! Ну, послал ответ, а там базарь, сколько хочешь, а счеток тихо мирно набегает...

Фрикинг определителей и автоответчиков

Первый способ обмана определителя действует только на старых моделях. Для этого надо позвонить на взламываемый определитель и, пока твой номер не определился, перейти в тоновый режим и набрать ложный номер.

Второй способ заключается в анонимном выходе на международную линию. Тут есть много способов. Можно послать прямо на линию через модем (когда прямой гудок) ноту «Ля» первой октавы длительностью 0,001 сек. Можно в HiperTerminal из Windows набрать команду ATDP8W15(095) для плохих линий или команду ATDP{0FH}(095) для обычных и хороших линий.

Есть еще команда ATDP8W!!!!!!!!!!!!!!!(095). 095 надо заменять на код города, куда надо позвонить. После команды должен стоять сам телефонный номер. Можно звонить таким способом и в другие страны, но тогда тебя выследят моментально. Можно еще записать звук нажатия кнопки 8 и совсем чуть-чуть изменить его в любом редакторе. Заметь, надо не применять эффекты, а изменять длину «полосочек». Можно записать чужой звук и потом звонить якобы с его телефона.

Насчет ноты «Ля». Это можно сделать с помощью программы SoundForge. Но там надо будет поставить в параметрах сигнал MF, длину 0,04, паузу и обрыв через 0,001. В поле dial string надо вписать 1*******. Вместо ******* надо вписать номер, от чьего имени ты будешь звонить в обратном порядке. Повторяющиеся символы заменяются на B. Дело в том, что всего при наборе номера звуки бывают 16-ти высот. Следовательно, 0123456789ABCDEF. Например, номер 123-66-99 будет выглядеть как 1B9B6321.

Есть способ в юзанье специальных программ для Internet-телефонии. Там все просто — оплачиваешь по левой кредитке и вперед. Причем, большинство сайтов, предоставляющих эту услугу, пропускают сгенерированные кредитки.

Теперь про автоответчики. Для того, чтобы захватить контроль над автоответчиком, надо позвонить на него, перейти в тоновый режим и набрать его код. Дело в том, что большинство юзеров автоответчиков настолько тупы, что не в состоянии сменить себе этот код. После того

как ты узнаешь модель автоответчика (для этого нужен подход к клиенту), узнай стандартный код для этой модели. Для этих целей и существуют магазины. Иди в любой магазин и попроси дать посмотреть мануал по нужной тебе модели. Вот код у тебя в руках. Функции автоответчика тоже можно узнать из мануала.

Теперь про таксофоны. Способов взломать — куча, но я тебе поведаю только об одном. Действует он только на телефоны фирмы УРМЕТ. Всовываешь карточку, снимаешь трубку, набираешь телефон, кладешь трубку, вытаскиваешь карточку, набираешь **0?. Вместо знака вопроса нужно набрать 1, 2 или 3. Без разницы. Этот способ не действует на некоторых АТС. Дело в том, что АТС запоминает последний набранный номер. Команда **0 вызывает повтор номера. Автомат нажатие * не различает, для автомата ты набрал 01/02/03. То есть АТС повторяет номер, а автомат думает, что ты звонишь в 01/02/03 и включает микрофон.

Технология изготовления магнитных карточек

В качестве примера рассмотрим таксофонную магнитную карту Urmet Patent. Таксофоны, использующие эти карты, имеются, в частности, во многих городах России. Карта представляет собой прямоугольник из упругого тонкого пластика, на который с одной стороны наносится полоска магнитного материала, с другой стороны — рекламная картинка. Левый верхний угол отрывной. Он играет роль пломбы, подтверждающей, что до вас этой картой никто не пользовался. Перед началом эксплуатации его удаляют.

Далее мы рассмотрим, как самостоятельно изготовить такую карту с применением немного необычной технологии. Пока не будем касаться вопроса схемотехники и конструкции устройства для чтения-записи информации, а поговорим о самой карточке. Считывание магнитной записи с карточки имеет свои особенности. В обычном магнитофоне лента плотно прижимается к головке специальной подпружиненной подушечкой и, к тому же, немного огибает головку. Это удается сделать, потому что лента очень тонкая и мягкая. С карточкой так не получится. Из-за того, что карточка жесткая и ее материал имеет некоторые остаточные неровности, не удается обеспечить идеальное прилегание считывающей головки к магнитному носителю. При сильном прижиме головки к карточке может возникнуть ее притормаживание в подающем тракте и возникнет сильный износ головки и носителя самой карточки. Поэтому реально головка практически не касается дорожки на карточке, находясь на микронном расстоянии от нее. Применяются либо обычные

индукционные головки, либо полупроводниковые магниточувствительные приборы. Карточку обычно носят в кошельке или кармане, где ее магнитный слой может поцарапаться, но нужно гарантировать клиенту устойчивое считывание карточки даже при наличии микродефектов. Все эти проблемы на практике решают, применяя достаточно толстый слой магнитного носителя, имеющего высокую коэрцитивность (способность к намагничиванию).

Для изготовления самодельной карточки нам понадобятся:

- Старые гибкие диски 5,25".
- Тонкий плотный картон.
- Самоклеящаяся бумага.
- Клей ПВА.
- Утюг и ножницы.

Нельзя просто приклеить полоску магнитного носителя, вырезанную из материала дискеты на кусок картона, так как крайне сложно нанести быстросохнущий клей очень тонким ровным слоем и аккуратно приклеить магнитную полоску так, чтобы клей не выступал из-под ее краев.

Таким образом, сначала делаем заготовку, по размеру близкую к карточке, но чуть больше. Берем тонкий картон, по толщине примерно, как маленький календарик. Но необходимо, чтобы у него была только одна глянцевая сторона, поэтому календарик не подойдет — ПВА плохо прилипнет. Берем импортную самоклеящуюся бумагу с отрывной основой. Такую цветную бумагу можно купить в магазине канцтоваров. Аккуратно смазываем клеем ПВА шершавую сторону картона и бумагу. Не испачкайте обратную сторону картона. Складываем намазанные слои, кладем заготовку на плотную ровную поверхность и через газетку проглаживаем утюгом. Утюг включаем на «шелк» или чуть горячее. Кто делал «дембельский альбом», уже натренирован в таком методе склеивания. Гладим с двух сторон. Через несколько минут бутерброд будет готов.

В случае, если его сильно коробит после остывания и не удается отгладить, значит картон не подходит. Попробуйте другой картон, можно вообще без глянца. Разберите дискету, вырежьте из нее полоску, равную по ширине заводской, но чуть длиннее. Из бумажной заготовки по образцу вырежьте саму карточку. Отслоите защитный слой от самоклеящейся бумаги и аккуратно приклейте в нужное место магнитную полоску. Перед этим вымойте руки и вообще будьте очень аккуратны. Малейшая соринка, попавшая под магнитную полоску, погубит вашу работу. Оторвать полоску обратно вы уже не сможете. Возьмите тонкую писчую

бумагу и подклейте встык к краям магнитной полоски. Подберите бумагу по толщине магнитной ленты. Не используйте кальку и подобную ей вощеную бумагу. Она может отклеиться от основы. Обрежьте излишки бумаги по краям. Бритвенным лезвием срежьте излишки магнитной полоски, сняв небольшую фасочку по краям. Удалите, при необходимости, заусенцы по краям карточки. Болванка для последующей записи готова. Метод не так сложен, как это может показаться, и позволяет делать болванки чуть ли не партиями.

ANAC-номер

ANAC (Automatic Number Announcement Circuit)-номер — это телефонный номер, который воспроизводит номер вызвавшего его телефона. ANAC-номера очень удобны в случае, если вам нужно узнать номер телефона из двухпроводной линии.

ANAC-номер и ваш регион

Как найти ваш ANAC-номер: в списке, помещенном ниже, отыщите ваш NPA (Код региона) и пробуйте набрать расположенный рядом с кодом номер. В случае, если это не получится, наберите 1 плюс номер, расположенный рядом с кодом. В случае, если и это не сработает, пробуйте набрать общий номер, к примеру 311, 958 и 200-222-2222. В случае, если вы найдете ANAC-номер своей области, пожалуйста, сообщите о нем нам.

Обратите внимание, что часто ANAC-номер неодинаков для различных моделей переключателей в одном и том же городе. Географические названия в списке НЕ полностью соответствуют зоне действия ANAC-номера, они (географические названия) предназначены только для удобства поиска.

Многие компании используют возможности номера «800», благодаря которым можно определить, с какого номера вам звонят. Большая часть из них подразумевает оперирование с несколькими меню для того, чтобы получить искомый номер телефона.

(800) 238-4959

Система голосовой электронной почты.

(800) 328-2630

Секс по телефону.

(800) 568-3197

Автоматизированная линия блокирования компании Info Access Telephone.

(800) 571-8859

Секс по телефону.

(800) 692-6447

(800) MY-ANI-IS.

(800) 455-3256

Неизвестная линия.

404-988-9664

Это не-«800» ANAC, работающий в масштабе всей страны. Единственное неудобство этого номера — то, что с ним можно связаться лишь через AT&T Carrier.

Access Code 10732

Другой общенациональный не-«800» ANAC — это номер Глена Роберта (Glen Robert) из Full Disclosure Magazine, 10555-1-708-356-9646.

Пожалуйста, по возможности пользуйтесь местными ANAC-номерами, поскольку неправильное обращение может уничтожить «800» ANAC-номера.

Внимание: приведенные здесь географические названия могут рассматриваться только как ссылки. ANAC-номера могут варьироваться в пределах одного и того же города.

NPA	ANAC номер	Район
201	958	Хакенсак/Джерси-сити/Ньюарк/Патерсон, Нью-Джерси
202	811	Округ Колумбия
203	970	Центральные области
205	300-222-2222	Бирмингем, Алабама
205	300-555-5555	Маленькие городки в Алабаме
205	300-648-1111	Дора, Алабама
205	300-765-4321	Бессемер, Алабама
205	300-798-1111	Форестдейл, Алабама
205	300-833-3333	Бирмингем, Алабама
205	557-2311	Бирмингем, Алабама
205	811	Пел-сити/Кропуел/Линкольн, Алабама
205	841-1111	Таррант, Алабама
205	908-222-2222	Бирмингем, Алабама

206	411	Вашингтон (восточный)
207	958	Мэн
209	830-2121	Стоктон, Калифорния
209	211-9779	Стоктон, Калифорния
210	830	Браунсвиль/Ларедо/Сан-Антонио, Техас
212	958	Манхеттен, Нью-Йорк
213	114	Лос-Анджелес, Калифорния (GTE)
213	1223	Лос-Анджелес, Калифорния
213	211-2345	Лос-Анджелес, Калифорния (English формат)
213	211-2346	Лос-Анджелес, Калифорния (DTMF формат)
213	760-2???	Лос-Анджелес, Калифорния (DMS ATC)
213	61056	Лос-Анджелес, Калифорния
214	570	Даллас, Техас
214	790	Даллас, Техас (GTE)
214	970-222-2222	Даллас, Техас
214	970-611-1111	Даллас, Техас (Southwestern Bell)
215	410-xxxx	Филадельфия, Пенсильвания
215	511	Филадельфия, Пенсильвания
215	958	Филадельфия, Пенсильвания
216	200-XXXX	Аркон/Кантон/Кливленд/Лорейн/Янгстаун, Огайо
216	331	Аркон/Кантон/Кливленд/Лорейн/Янгстаун, Огайо
216	959-9892	Аркон/Кантон/Кливленд/Лорейн/Янгстаун, Огайо
217	200-xxx-xxxx	Чэмпейн-Урбана/Спрингфилд, Иллинойс
219	550	Гэри/Хаммонд/Мичиган/Саубенд, Индиана
219	559	Гэри/Хаммонд/Мичиган/Саубенд, Индиана
301	958-9968	Хейгерстаун/Роксвиль, Мэриленд
310	114	Лонг Бич, Калифорния (многие GTE ATC)
310	1223	Лонг Бич, Калифорния (какая-то 1AESS ATC)
310	211-2345	Лонг Бич, Калифорния (English формат)
310	211-2346	Лонг Бич, Калифорния (DTMF формат)
312	200	Чикаго, Иллинойс
312	290	Чикаго, Иллинойс
312	1-200-8825	Чикаго, Иллинойс
312	1-200-5551212	Чикаго, Иллинойс
313	200-200-2002	Анн Арбор/Дирборн/Детройт, Мичиган
313	200-222-2222	Анн Арбор/Дирборн/Детройт, Мичиган
313	200-xxx-xxxx	Анн Арбор/Дирборн/Детройт, Мичиган
313	2002002002000	Анн Арбор/Дирборн/Детройт, Мичиган

314	410-xxxx#	Колумбия/Джефферсон-сити/Сент-Льюис, Миссури
315	953	Сиракьюс/Отика, Нью-Йорк
315	958	Сиракьюс/Отика, Нью-Йорк
315	998	Сиракьюс/Отика, Нью-Йорк
317	310-222-2222	Индианаполис/Кокомо, Индиана
317	559-222-2222	Индианаполис/Кокомо, Индиана
317	743-1218	Индианаполис/Кокомо, Индиана
334	5572411	Монтгомери, Алабама
334	5572311	Монтгомери, Алабама
401	200-200-4444	Род-Айленд
401	222-2222	Род-Айленд
402	311	Линкольн, Новая Англия
404	311	Атланта, Джорджия
404	940-xxx-xxxx	Атланта, Джорджия
404	990	Атланта, Джорджия
405	890-7777777	Энид/Оклахома, Оклахома
405	897	Энид/Оклахома, Оклахома
407	200-222-2222	Орландо/Уэст-Палм-Бич, Флорида
408	300-xxx-xxxx	Сан-Хосе, Калифорния
408	760	Сан-Хосе, Калифорния
408	940	Сан-Хосе, Калифорния
409	951	Бомонт/Галвестон, Техас
409	970-xxxx	Бомонт/Галвестон, Техас
410	200-6969	Анаполис/Балтимор, Мэриленд
410	200-555-1212	Анаполис/Балтимор, Мэриленд
410	811	Анаполис/Балтимор, Мэриленд
412	711-6633	Питтсбург, Пенсильвания
412	711-4411	Питтсбург, Пенсильвания
412	999-xxxx	Питтсбург, Пенсильвания
413	958	Питтсвил/Спрингфилд, Миннесота
413	200-555-5555	Питтсвил/Спрингфилд, Миннесота
414	330-2234	Фон-дю-Лак/Грин Бей/Милуоки/Расин, Висконсин
415	200-555-1212	Сан-Франциско, Калифорния
415	211-2111	Сан-Франциско, Калифорния
415	2222	Сан-Франциско, Калифорния
415	640	Сан-Франциско, Калифорния
415	760-2878	Сан-Франциско, Калифорния
415	7600-2222	Сан-Франциско, Калифорния
419	311	Толедо, Огайо
502	2002222222	Франкфорт/Луисвиль/Педака/Шелбивилл, Кентукки

502	997-555-1212	Франкфорт/Луисвиль/Педака/Шелбивилл, Кентукки
503	611	Портланд, Орегон
503	999	Портланд, Орегон (GTE)
504	99882233	Батон-Руж/Новый Орлеан, Луизиана
504	201-269-1111	Батон-Руж/Новый Орлеан, Луизиана
504	998	Батон-Руж/Новый Орлеан, Луизиана
504	99851-0...0	Батон-Руж/Новый Орлеан, Луизиана
508	958	Фол Ривер/Нью Бедфорд/Ворчестер, Миннесота
508	200-222-1234	Фол Ривер/Нью Бедфорд/Ворчестер, Миннесота
508	200-222-2222	Фол Ривер/Нью Бедфорд/Ворчестер, Миннесота
508	26011	Фол Ривер/Нью Бедфорд/Ворчестер, Миннесота
509	560	Спокан/Уолла-Уолла/Якима, Вашингтон
510	760-1111	Окленд, Калифорния
512	830	Остин/Корпус-Кристи, Техас
512	970-xxxx	Остин/Корпус-Кристи, Техас
515	5463	Де-Мойн, Айова
515	811	Де-Мойн, Айова
516	958	Хемпстед/Лонг-Айленд, Нью-Йорк
516	968	Хемпстед/Лонг-Айленд, Нью-Йорк
517	200-222-2222	Бей-Сити/Джексон/Лансинг, Мичиган
517	2002002002200	Бей-Сити/Джексон/Лансинг, Мичиган
518	511	Олбани/Шенектади/Трой, Нью-Йорк
518	997	Олбани/Шенектади/Трой, Нью-Йорк
518	998	Олбани/Шенектади/Трой, Нью-Йорк
603	200-222-2222	Нью-Гемпшир
606	997-555-1212	Эшланд/Винчестер, Кентукки
606	711	Эшланд/Винчестер, Кентукки
607	993	Бингемтон/Элмайра, Нью-Йорк
609	958	Атлантик-сити/Камден/Трентон/Вайнленд, Нью-Джерси
610	958	Аллентайн/Рединг, Пенсильвания
610	958-4100	Аллентайн/Рединг, Пенсильвания
612	511	Миннеаполис/Сент-Пол, Миннесота
614	200	Колумбус/Стубенвиль, Огайо
614	571	Колумбус/Стубенвилл, Огайо
615	2002002200200	Чаттануга/Ноксвилл/Нашвилл, Теннесси
615	2002222222	Чаттануга/Ноксвилл/Нашвилл, Теннесси
615	830	Нашвилл, Теннесси

616	200-222-2222	Батл-Крик/Гранд-Рапидс/Каламазу, Мичиган
617	200-222-1234	Бостон, Массачусетс
617	200-222-2222	Бостон, Массачусетс
617	200-444-4444	Бостон, Массачусетс (Вобурн, Массачусетс)
617	220-2622	Бостон, Массачусетс
617	958	Бостон, Массачусетс
618	200-xxx-xxxx	Олтон/Каиро/Монтвернон, Иллинойс
618	930	Олтон/Каиро/Монтвернон, Иллинойс
619	211-2001	Сан-Диего, Калифорния
619	211-2121	Сан-Диего, Калифорния
703	811	Александрия/Арлингтон/Роанок, Виргиния
704	311	Ашвилл/Шарлотт, Северная Каролина
707	211-2222	Уайрека, Калифорния
708	1-200-5551212	Чикаго/Элджин, Иллинойс
708	1-200-8825	Чикаго/Элджин, Иллинойс
708	200-6153	Чикаго/Элджин, Иллинойс
708	724-9951	Чикаго/Элджин, Иллинойс
708	356-9646	Чикаго/Элджин, Иллинойс
713	380	Хьюстон, Техас
713	970-xxxx	Хьюстон, Техас
713	811	Хамбле, Техас
714	114	Анахейм, Калифорния (GTE)
714	211-2121	Анахейм, Калифорния (PacBell)
714	211-2222	Анахейм, Калифорния (Pacbell)
716	511	Буффало/Ниагара-Фолс/Рочестер, Нью-Йорк (Rochester Tel)
716	990	Буффало/Ниагара-Фолс/Рочестер, Нью-Йорк (Rochester Tel)
717	958	Гаррисберг/Скрантон/Уилкс-Барре, Пенсильвания
718	958	Бронкс/Бруклин/Статен Айленд
802	2-222-2222222	Вермонт
802	200-222-2222	Вермонт
802	1-700-2222222	Вермонт
802	111-2222	Вермонт
805	114	Бейкерсфилд/Санта Барбара, Калифорния
805	211-2345	Бейкерсфилд/Санта Барбара, Калифорния
805	211-2346	Бейкерсфилд/Санта Барбара, Калифорния (Returns DTMF)
805	830	Бейкерсфилд/Санта Барбара, Калифорния
806	970-xxxx	Амарилло/Лаббок, Техас

810	2002002002200	Флинт/Понтиак/Саутфилд/Трой, Мичиган
812	410-555-1212	Эвансвилл, Индиана
813	311	Форт-Майерс/Сент-Питерсберг/Тампа, Флорида
815	200-xxx-xxxx	Ла-Саль/Рокфорд, Иллинойс
815	290	Ла-Саль/Рокфорд, Иллинойс
817	211	Форт-Уэрт/Уэйко, Техас
817	970-611-1111	Форт-Уэрт/Уэйко, Техас (Southwestern Bell)
818	1223	Пасадена, Калифорния (ряд 1AESS ATC)
818	211-2345	Пасадена, Калифорния (English формат)
818	211-2346	Пасадена, Калифорния (DTMF формат)
903	970-611-1111	Тайлер, Техас
904	200-222-222	Джексонвилл/Пенсакола/Таллахасси, Флорида
906	1-200-2222222	Марикетт/Су-Сент-Мари, Мичиган
907	811	Аляска
908	958	Нью-Брансуик, Нью-Джерси
910	200	Файеттвилл/Гринсборо/Роли/Уинстон-Сейлем, Северная Каролина
910	311	Файеттвилл/Гринсборо/Роли/Уинстон-Сейлем, Северная Каролина
910	988	Файеттвилл/Гринсборо/Роли/Уинстон-Сейлем, Северная Каролина
914	990-1111	Пикскилл/Покипси/Уайт-Плейнс/Йонкерс, Нью-Йорк
915	970-xxxx	Абилин/Эль Пасо, Техас
916	211-2222	Сакраменто, Калифорния (Pac Bell)
916	461	Сакраменто, Калифорния (Roseville Telepohone)
919	200	Дарем, Северная Каролина
919	711	Дарем, Северная Каролина

Канада:

204	644-4444	Манитоба
306	115	Саскачеван
403	311	Альберта, Юкон и Северо-западные территории
403	908-222-2222	Альберта, Юкон
403	999	Альберта, Юкон
416	997-xxxx	Торонто, Онтарио
506	1-555-1313	Нью-Брансуик
514	320-xxxx	Монреаль, Квебек
519	320-xxxx	Лондон, Онтарио

604	1116	Британская Колумбия
604	1211	Британская Колумбия
604	211	Британская Колумбия
613	320-2232	Оттава, Онтарио
705	320-4567	Норт-Бэй/Су-Сент-Мари, Онтарио

Австралия:

+61	03-552-4111	Провинция Виктория
+612	19123	Все главные города страны

Великобритания:

175

Израиль:

110

Ringback-номер

Ringback-номер — номер, при соединении с которым сигнал вызова немедленно вернется к телефону, с которого был сделан звонок.

В большинстве случае вы вызываете ringback-номер, быстро вешаете трубку и через небольшой промежуток времени снимаете ее опять. Так вы выбираетесь из ловушки, и в трубке будут слышаться различные звуки. После этого вы можете отключиться. Через несколько секунд вам позвонят.

Ringback-номер и ваш регион

В приводимом ниже списке «x» означает «вставьте соответствующие цифры из номера, с которого вы звоните». «?» означает, что номер варьируется в регионе от АТС к АТС или время от времени меняется. Попробуйте все возможные комбинации.

В случае, если в списке нет ringback для вашего NPA, попробуйте общие номера типа 951-xxx-xxxx, 954, 957 и 958. Также можно попробовать номера, приведенные для другой NPA, обслуживаемой вашей же телефонной компанией.

Внимание: приведенные здесь географические названия могут рассматриваться только как ссылки. ANAC-номера могут варьироваться в пределах одного и того же города.

NPA	Ringback-номер	Регион
201	55?-xxxx	Хакенсак/Джерси-сити/Ньюарк/ Патерсон, Нью-Джерси
202	958-xxxx	Округ Колумбия

203	99?-xxxx	Центральный район
206	571-xxxx	Вашингтон
208	99xxx-xxxx	Айдахо
213	1-95x-xxxx	Лос-Анджелес, Калифорния
215	811-xxxx	Филадельфия, Пенсильвания
216	551-xxxx	Аркон/Кантон/Кливленд/ Лорейн/Янгстаун, Огайо
219	571-xxx-xxxx	Гэри/Хаммонд/Мичиган/Саубенд, Индиана
219	777-xxx-xxxx	Гэри/Хаммонд/Мичиган/ Саубенд, Индиана
301	579-xxxx	Хейгерстаун/Роксвиль, Мэриленд
301	958-xxxx	Хейгерстаун/Роксвиль, Мэриленд
303	99X-xxxx	Гранд-Джанкшен, Колорадо
304	998-xxxx	Западная Виргиния
305	999-xxxx	Форт-Лодердейл/Ки-Уэст/Майами, Флорида
312	511-xxxx	Чикаго, Иллинойс
312	511-xxx-xxxx	Чикаго, Иллинойс
312	57?-xxxx	Чикаго, Иллинойс
315	98x-xxxx	Сиракьюс/Отика, Нью-Йорк
317	777-xxxx	Индианаполис/Кокомо, Индиана
317	yyy-xxxx	Индианаполис/Кокомо, Индиана
319	79x-xxxx	Давенпорт/Дубьюк, Айова
334	901-xxxx	Монтгомери, Алабама
401	98?-xxxx	Род-Айленд
404	450-xxxx	Атланта, Джоджия
407	988-xxxx	Орландо/Уэст-Палм-Бич, Флорида
412	985-xxxx	Питтсбург, Пенсильвания
414	977-xxxx	Фон-дю-Лак/Грин Бей/Милуоки/Расин, Висконсин
414	978-xxxx	Фон-дю-Лак/Грин Бей/Милуоки/Расин, Висконсин
415	350-xxxx	Сан-Франциско, Калифорния
417	551-xxxx	Джоплин/Спрингфилд, Миссури
501	221-xxx-xxxx	Арканзас
501	721-xxx-xxxx	Арканзас
502	988	Франкфорт/Луисвиль/Педака/ Шелбивилл, Кентукки
503	541-XXXX	Орегон
504	99x-xxxx	Батон-Руж/Новый Орлеан, Луизиана
504	9988776655	Батон-Руж/Новый Орлеан, Луизиана
512	95X-xxxx	Остин, Техас

U 513	951-xxxx	Цинциннати/Дейтон, Огайо
513	955-xxxx	Цинциннати/Дейтон, Огайо
U 513	99?-xxxx	Цинциннати/Дейтон, Огайо (X = 0, 1, 2, 3, 4, 8 или 9)
516	660-xxx-xxxx	Хемпстед/Лонг-Айленд, Нью-Йорк
601	777-xxxx	Миссисипи
609	55?-xxxx	Атлантик-сити/Камден/Трентон/ Вайнленд, Нью-Джерси
610	811-xxxx	Аллентайн/Рединг, Пенсильвания
612	511	Миннеаполис/Сент-Пол, Миннесота
612	999-xxx-xxxx	Миннеаполис/Сент-Пол, Миннесота
614	998-xxxx	Колумбус/Стубенвиль, Огайо
615	920-XXXX	Чаттануга/Ноксвилл/Нашвилл, Теннесси
615	930-xxxx	Чаттануга/Ноксвилл/Нашвилл, Теннесси
616	946-xxxx	Батл-Крик/Гранд-Рапидс/Каламазу, Мичиган
619	331-xxxx	Сан-Диего, Калифорния
619	332-xxxx	Сан-Диего, Калифорния
703	958-xxxx	Александрия/Арлингтон/Роанок, Виргиния
708	511-xxxx	Чикаго/Элджин, Иллинойс
714	330?	Анахейм, Калифорния (GTE)
714	33?-xxxx	Анахейм, Калифорния (PacBell)
716	981-xxxx	Рочестер, Нью-Йорк (Rochester Tel)
718	660-xxxx	Бронкс/Бруклин/Квинс/Статен Айленд, Нью-Йорк
719	99x-xxxx	Колорадо Спирнгс/Лидвилл/Пуэбло, Колорадо
801	938-xxxx	Юта
801	939-xxxx	Юта
802	987-xxxx	Вермонт
804	260	Шарлоттесвил/Ньюпорт-Ньюс/Норфолк/ Ричмонд, Виргиния
805	114	Бейкерсфилд/Санта Барбара, Калифорния
805	980-xxxx	Бейкерсфилд/Санта Барбара, Калифорния
810	951-xxx-xxxx	Понтиак/Саутфилд/Трой, Мичиган
813	711	Форт-Майерс/Сент-Питерсберг/Тампа, Флорида
817	971	Форт-Уэрт/Уэйко, Техас

906	951-xxx-xxxx	Марикетт/Су-Сент-Мари, Мичиган
908	55?-xxxx	Нью-Брансуик, Нью-Джерси
908	953	Нью-Брансуик, Нью-Джерси
913	951-xxxx	Лоуренс/Салайна/Топика, Канзас
U 914	660-xxxx-xxxx	Пикскилл/Покипси/Уайт-Плейнс/ Йонкерс, Нью-Йорк

Канада:

204	590-xxx-xxxx	Манитоба
416	57x-xxxx	Торонто, Онтарио
416	99x-xxxx	Торонто, Онтарио
416	999-xxx-xxxx	Торонто, Онтарио
506	572 + xxx-xxxx	Нью-Брансуик
514	320-xxx-xxxx	Монреаль, Квебек
519	999-xxx-xxxx	Лондон, Онтарио
613	999-xxx-xxxx	Оттава, Онтарио
705	999-xxx-xxxx	Норт-Бэй/Су-Сент-Мари, Онтарио

Австралия:

+ 61 199

Бразилия:

109 или 199

Голландия:

99-xxxxxx

Новая Зеландия:

137

Швеция:

0058

Великобритания:

174 или 1744 или 175 или 0500-89-0011

Loop

Loop — это пара телефонных номеров, обычно последовательных, подобно 836-9998 и 836-9999. Они используются телефонной компанией для тестирования. Что же хорошего могут дать нам loop'ы? Что ж, они полезны по многим параметрам. Вот простой пример использования loop'а.

Каждый loop имеет два конца, «высокий» и «низкий». Один конец дает (обычно) постоянный, громкий тон, когда это **Вызываемый**. Другой конец тих. Обычно loop не звонит одновременно. Когда сигнал поступает одновременно к **обоим** концам, звонящие на каждый из концов loop'а

люди могут беседовать через loop друг с другом. На некоторых loop'ах установлены речевые фильтры и они не пропускают ничего, кроме постоянного тона; от них вам будет мало толку. А нужны loop'ы вот для чего: вы можете использовать рабочие loop'ы для мелкого хулиганства с телефонными счетами! Сначала позвоните на тот конец, который дает громкий тон. Затем, если оператор или кто-то другой вызовет другой конец, тон станет тише. Дальше действуйте, как если бы просто зазвонил телефон и вы сняли трубку... скажите «Привет», «Алло», «Чу», «Ё-мое» или что еще вам взбредет в голову. Оператор просто решит, что не туда попал, и все! Теперь счет телефона пойдет по loop'у, и его получит ваш локальный RBOC! Попробуйте использовать эту методику периодически. Loop может оказаться полезен в случае, когда вам нужно пообщаться с кем-то, кому вы не хотите давать номер своего телефона.

CNA-номер

CNA — это сокращение от Customer Name and Address. CNA-номер — справочный номер, используемый сотрудниками телефонных компаний для определения имени и адреса хозяина телефонного аппарата. В случае, если оператор телефонной сети обнаружит незарегистрированную линию, то он сможет обратиться к ANI-номеру и определить номер телефона-нарушителя, а затем вызвать оператора CNA и узнать имя владельца и его адрес.

Обычные CNA-номера доступны только сотрудникам телефонных компаний. Частные граждане могут легально получить предоставляемую системой CNA информацию, прибегнув к услугам частных компаний. Их две:

- Unidirectory (900) 933-3330
- Telename (900) 884-1212

Обратите внимание, что телефоны компаний начинаются с (900) и, следовательно, будут вам стоить примерно $1 в минуту.

В случае, если вы житель 312-го или 708-го регионов, то вы можете обратиться в компанию AmeriTech, предоставляющей услуги CNA широкой публике. Ее номер — 796-9600. Стоимость одного звонка — $35; за один раз вы можете запросить информацию о двух номерах.

Если вы живете в 415-м регионе, то здесь свободный доступ к системе CNA обеспечивается компанией Pacific Bell по телефону (415) 781-5271.

Телефонная компания, услуги CNA и ваш регион

- 203 (203) 771-8080 Центральный район
- 312 (312) 796-9600 Чикаго, Иллинойс
- 506 (506) 555-1313 Нью-Брансуик
- 513 (513) 397-9110 Цинцинати/Дейтон, Огайо
- 516 (516) 321-5700 Хемпстед/Лонг-Айленд, Нью-Йорк
- 518 (518) 471-8111 Олбани/Шенектади/Трой, Нью-Йорк
- 614 (614) 464-0123 Колумбус/Стубенвиль, Огайо
- 813 (813) 270-8711 Форт-Майерс/Сент-Питерсберг/Тампа, Флорида

Какие телефонные номера всегда «заняты»?

216	xxx-9887	Аркон/Кантон/Кливленд/Лорейн/Янгстаун, Огайо
303	431-0000	Денвер, Колорадо
303	866-8660	Денвер, Колорадо
316	952-7265	Додж-Сити/Уичита, Канзас
501	377-99xx	Арканзас
719	472-3773	Колорадо Спирнгс/Лидвилл/Пуэбло, Колорадо
805	255-0699	Бейкерсфилд/Санта Барбара, Калифорния
818	885-0699	Пасадена, Калифорния
906	632-9999	Марикетт/Су-Сент-Мари, Мичиган
906	635-9999	Марикетт/Су-Сент-Мари, Мичиган
914	576-9903	Пикскилл/Покипси/Уайт-Плейнс/Йонкерс, Нью-Йорк

Какие номера периодически разъединяют телефонное соединение?

314	511	Колумбия/Джефферсон-сити/Сент-Луис, МО (1 минута)
404	420	Атланта, Джорджия (5 минут)
405	953	Энид/Оклахома, Оклахома (1 минута)
407	511	Орландо/Уэст-Палм-Бич, Флорида (1 минута)
512	200	Остин/Корпус Кристи, Техас (1 минута)
516	480	Хемпстед/Лонг-Айленд, Нью-Йорк (1 минута)
603	980	Нью-Гемпшир

614	xxx-9894	Колумбус/Стубенвиль, Огайо
805	119	Бейкерсфилд/Санта Барбара, Калифорния (3 минуты)
919	211 или 511	Дарем, Северная Каролина (10 минут – 1 час)

Proctor Test Set

Proctor Test Set — это устройство, используемое telco personell для диагностики телефонных линий. Вы набираете номер Proctor Test Set, нажимаете кнопки на тоновом номеронабирателе и выбираете необходимый вам тест.

Proctor Test Set и ваш регион

805	111	Бейкерсфилд/Санта Барбара, Калифорния
909	117	Тайлер, Техас
913	611-1111	Лоуренс/Салайна/Топика, Канзас

Scanning

Scanning — это набор большого количества телефонных номеров с целью обнаружения интересующего человека (или компьютера) или тона. Scanning может выполняться вручную, хотя набор нескольких тысяч номеров вручную — чрезвычайно утомительная работа, отнимающая много времени.

Лучше использовать специальную scanning-программу, иногда называемую «war dialer» или «demon dialer». В настоящее время лучшей из доступных пользователям PC-DOS scanning-программ является ToneLoc, созданная Minor Threat и Mucho Maas. ToneLoc можно скачать с ftp.paranoia.com /pub/toneloc/.

«War dialer» набирает телефонные номера и регистрирует их ответы в журнале. Вы же потом просто выбираете номера, помеченные как «carry» или «tone».

Законно ли использование scanning-программ?

Обвинить кого-либо в использовании этих программ достаточно сложно, так как если нарушитель соединится с каким-то номером всего лишь раз, его будет невозможно определить. Невозможно даже представить себе толпу тех, до кого дозвонился компьютер со scanning-программой, преследующую нарушителя спокойствия. Известно, правда, что некоторые офисы телефонных компаний странно реагируют на использование scanning-программ. Иногда после того, как начато сканирование, оказывается, что ваш телефон на несколько часов отключен. Впрочем, это необязательно. Лучше всего, конечно, сначала выяснить, не подпадают ли ваши действия под какой-нибудь дурацкий закон, запрещающий этот вид деятельности. В случае, если же такого закона нет, то единственный способ выяснить, что же произойдет, это начать сканирование.

DTMF-частоты

DTMF — сокращение от Dual Tone Multi Frequency. Эти частоты — те тона, которые вы слышите, нажимая какую-нибудь кнопку на своем телефоне. Тон кнопки — сумма тонов строки и столбца. Клавиш A, B, C и D на стандартных телефонах не существует.

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	*	D

Частоты телефонных тонов

Тип	Hz	On	Off
Тон набора номера	350 и 440	---	---
Сигнал «занято»	480 и 620	0.5	0.5
Потеря при перегрузке	480 и 620	0.2	0.3
Обратный звонок (норм.)	440 и 480	2.0	4.0
Обратный звонок (PBX)	440 и 480	1.5	4.5
Переназначение локальное	480 и 620	3.0	2.0
Неправильно набран номер	200 и 400		
Предупреждение о скором рассоединении	1400 и 2060	0.1	0.1
Рассоединение	2450 и 2600	---	---

LASS-коды

Ниже приводим список стандартных кодов Local Area Signalling Services (LASS) и Custom Calling Feature Control Codes (в различных регионах они могут быть незначительно изменены):

Услуга	Тон	Pulse/rotary	Примечание
Помощь/полиция	*12	n/a	[1]
Отмена пересылки	*30	n/a	[C1]
Автоматическая пересылка	*31	n/a	[C1]
Сообщите	*32	n/a	[C1] [2]
Кольцо селекторной связи 1(..)	*51	1151	[3]
Кольцо селекторной связи 2 (..)	*52	1152	[3]
Кольцо селекторной связи 3 (..)	*53	1153	[3]
Хранение Расширения	*54	1154	[3]
Заказчик инициировал след	*57	1157	
Выборочное отклонение обращения (или Экран Обращения)	*60	1160	
Выборочная различная тревога	*61	1161	
Выборочное принятие вызова	*62	1162	
Выборочная пересылка обращения	*63	1163	
ICLID активация	*65	1165	
Вызовите возврат (исходящий)	*66	1166	
Дисплей номера, блокирующий	*67	1167	[4]
Компьютерное ограничение доступа	*68	1168	
Вызовите возврат (входящий)	*69	1169	
Ожидание обращения отключает	*70	1170	[4]
Низкая передача обращения ответа	*71	1171	
Использование чувствительных способов прозвона	*71	1171	
Пересылка обращения (начало)	*72/72#	1172	
Пересылка обращения (отмена)	*73/73#	1173	
Быстрый набор (8 номеров)	*74/74#	1174	
Быстрый набор (30 номеров)	*75/75#	1175	

Анонимное отклонение обращения	*77	1177	[5] [M:*58]
Отключение экрана обращения (или вызов экрана)	*80	1160	[M:*50]
Различные выборочные отключения	*81	1161	[M:*51]
Выборочное отключение приема	*82	1162	
Выборочное отключение пересылки	*83	1163	[M:*53]
Отключение ICLID	*85	1165	
Вызов возврата (отмена снаружи)	*86	1186	[6] [M:*56]
Отмена обращения	*87	1187	[5] [M:*68]
Вызов возврата (внутр. отмена)	*89	1189	[6] [M:*59]

Счета:

(C1)

Означает, что код используется для обслуживания одной ячейки.

(1)

Для ячеек в Питтсбурге и для PA A/C 412 в некоторых других областях.

(2)

Показывает, что вы не местный и (не всегда) ваш номер.

(3)

Находится на территории Пак Бэлл; селекторный вызов вызывает отличительный звонок, который будет сгенерирован на электрической линии; удерживает линию, пока не будет поднята трубка на параллельном аппарате.

(4)

Применяется единожды, перед каждым звонком.

(5)

A.C.R.-блоки вызванивают тех, кто блокировал ID вызывающего оператора (используется на некоторых территориях).

(6)

Отменяет дальнейшие попытки возврата.

(M:*xx)

Альтернативный код, используемый для MLVP (multi-line variety package) Bellcore. Действует под различными именами в различных RBOC'ax. В системе Bellsouth, к примеру, именуется Prestige. Это — соглашение, аналогичное ЭССЕКС, для одиночных или множественных небольших групп телефонных линий.

Причина различия кодов для некоторых операций в MLVP состоит в том, что коду call-pickup соответствует — *8 в MLVP, так что все *8x коды перекодируются в *5x.

На каких частотах работают беспроводные телефоны

Ниже помещаем список частот, на которых работают телефоны 46/49 MHz первого поколения.

Канал	Переносной передатчик	Стационарный передатчик
1	49.670 MHz	46.610 MHz
2	49.845	46.630
3	49.860	46.670
4	49.770	46.710
5	49.875	46.730
6	49.830	46.770
7	49.890	46.830
8	49.930	46.870
9	49.990	46.930
10	49.970	46.970

Новые беспроводные телефоны на 900 MHz работают в следующем диапазоне частот: от 902 до 228 MHz, с каналом, располагающим между 30–100 KHz.

Caller-ID

Calling Number Delivery (CND), более известный как Caller-ID, — это вид телефонного обслуживания для частных клиентов и предприятий малого бизнеса. Caller-ID позволяет обращаться к Customer Premises Equipment (CPE) для получения номера стороны вызова и даты/времени

обращения в течение первого четырехсекундного интервала во время звонка.

Параметры

Данные выводятся на экран по следующим дефинициям:

Link Type (тип связи)

2-wire, simplex (двухпроводная, симплексная)

Transmission Scheme (схема передачи)

Analog, phase-coherent FSK (Аналог, фаза-когерентный FSK)

```
Logical 1 (mark)                1200 ± 12 Hz
Logical 0 (space)               2200 ± 22 Hz
Transmission Rate:              1200 bps
```

Transmission Level (уровень передачи)

13.5 ± dBm into 900 ohm load

Протокол

Протокол использует 8-разрядные слова (байты), каждый из которых ограничен начальным и стоповым битами. CND-сообщение использует перечисленные ниже форматы Single Data Message.

Channel Siezure Signal

Захват канала — это 30 продолжающихся байтов 0x55H (01010101), обеспечивающих обнаруживаемые альтернативные функции CPE (то есть буферирование данных для модема).

Carrier Signal

Этот сигнал состоит из 130 ± 25 MS метки (1200 Hz) для создания условий для приемника данных.

Message Type Word

Показывает параметры обслуживания и совместимости с сообщением данных. Слово типа сообщения для CND — 0x04H (00000100).

Message Length Word

Определяет общее число последовательных слов данных.

Data Words

Data Words (слова данных) закодированы в ASCII и содержат следующую информацию:

- Первые два слова обозначают месяц.
- Следующие два слова обозначают день месяца.
- Следующие два слова обозначают час по местному времени.
- Следующие два слова обозначают минуту после часа.
- Последующие слова, расположенные в поле данных, обозначают номер стороны вызова.

В случае, если номер стороны вызова не доступен из центрального офиса, поле данных будет содержать ASCII-символ «O».

В случае, если вызывающая сторона запрашивает возможности системы безопасности, поле данных будет содержать ASCII-символ «P».

Checksum Word

Содержит дополнение в двоичной системе исчисления по модулю 256 суммы других слов в сообщении (то есть message type, message length и data words). Принимающее оборудование получения может вычислять по модулю 256 суммы полученных слов и добавить эту сумму к checksum word. Результат, равный нулю, обычно указывает на то, что сообщение было получено правильно. Повторная передача сообщения не производится.

Вот пример полученного CND-сообщения, начинающегося с message type word:

```
04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51
04h= Calling number delivery information code (message type word)
12h= 18 decimal; Number of data words (date,time, and directory
number words)
ASCII 30,39= 09; September
ASCII 33,30= 30; 30th day
ASCII 31,32= 12; 12:00 PM
ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)
ASCII 36,30,39,35,35,35,31,32,31,32= (609) 555-1212; calling
party's directory number
51h= Checksum Word
```

Запрос Data Access Arrangement (DAA)

Для того чтобы обеспечить получение CND-информации, модем должен проверить телефонную линию между первым и вторым кольцевым пакетом в обход DAA, чтобы в прямом смысле избежать ловушки, которая блокировала бы передачу CND местным центральным ведомством. Простая модификация существующей DAA-схемы поможет легко справиться с этой задачей.

Требования к модему

Хотя данные, указывающие параметры интерфейса соответствуют спецификации на модемы Bell 202, для считывания CPE не обязательно иметь Бэлл 202 модем. A V. 23 1200 бит/сек модем может использоваться для демодуляции Бэлл 202 сигналов.

Бит индикации звонка на модеме может быть использован для мониторинга телефонной линии на предмет CND информации. После того, как установлен бит RI, указывающий на первый звонок, главная ЭВМ ждет момента, кода этот бит опять сбросится.

Главная ЭВМ затем конфигурирует модем, чтобы контролировать телефонную линию на предмет CND информации.

Передача сигналов

Согласно спецификации Bellcore, CND передача старт-сигналов начинается через 300 MS после первого звонка и стоп-сигналов по крайней мере за 475 MS до второго звонка.

Приложения

Получив однажды CND-информацию, пользователь может обрабатывать информацию множеством способов.

1. Дата, время и номер стороны вызова могут быть индицированы.

2. Используя поисковую таблицу, можно определить настоящее имя, скрывающееся за номером стороны вызова; эта информация также индицируется.

3. CND-информацию можно еще использовать следующими способами:

- Как приложения на доске объявлений.
- Помещение в черный список приложений.
- Для хранения пользовательского журнала системы.
- В качестве поддержки базы данных телемаркетинга.

Как блокировать Caller-ID

Прежде чем приступить к выполнению одного из представленных ниже вариантов блокировки Caller-ID, обязательно все тщательно про-

верьте. Некоторые из публикуемых способов прекрасно работают в одном регионе и не дают никакого результата в другом.

- Наберите *67 прежде, чем набирать основной номер (141 в Великобритании).
- Наберите номер локального TelCo и пусть он установит блок Caller-ID на используемой линии.
- Наберите 0 и попросите оператора вам перезвонить.
- Наберите обращение, используя предварительно оплаченную телефонную карточку.
- Наберите номер через Security Consultants (консультантов защиты) службы (900) PREVENT, если звонок внутри страны (имеются в виду США; $1,99 в минуту) или (900) STONEWALL, если звонок международный ($3,99/minute).

Безбоязненно и бесплатно используйте таксофон по назначению.

PBX

PBX расшифровывается как Private Branch Exchange.

PBX — маленькая АТС, принадлежащая компании или организации. Скажем, в фирме работает тысяча человек. Без PBX вы должны были бы установить тысячу телефонных линий. Однако только 10% сослуживцев говорит по телефону одновременно. Представьте, что у вас есть компьютер, который автоматически находит свободную внешнюю линию каждый раз, когда кто-то из ваших коллег снимает трубку. Используя подобную систему, вы могли бы оплачивать только 100 телефонных линий вместо 1000. Это и есть PBX.

VMB

VMB — это аббревиатура от Voice Mail Box. VMB представляет собой компьютер, который действует как автоответчик и эксплуатируется сотнями или тысячами пользователей. Каждый пользователь регистрирует в системе свой собственный Voice Mail Box (речевой почтовый ящик). Каждый почтовый ящик имеет номер и пароль для входа.

Без пароля вы можете только оставлять сообщения, адресованные пользователям VMB-системы. С паролем вы сможете читать сообщения и получите доступ к управлению почтовым ящиком. Часто почтовые

ящики создаются по умолчанию, встречаются также заброшенные ящики, которые больше не используются своим хозяином. К ним можно попробовать подобрать пароль. Бывает, что пароль соответствует номеру почтового ящика или представляет собой простую комбинацию цифр типа 1234.

Зачем нужны ABCD тоны

ABCD тоны — это просто дополнительные DTFM тоны, которые могут использоваться так же, как и стандартные (0–9). ABCD тоны используются в военной телефонной сети США (AutoVon), в некоторых ACD-системах (Automatic Call Distributor), для генерирования сообщений управления в некоторых PBX-системах и в некоторых любительских автоматических радиореаниматорах.

В сети AutoVon специальные телефоны оборудованы клавишами ABCD.

За этими клавишами определены значения:

- A — Срочная передача.
- B — Приоритет отмены срочной передачи.
- C — Приоритетная связь.
- D — Приоритетная отмена.

Разовое использование встроенного режима поддержки ACD-системы операторами Directory Assistance позволит вам объединить двух любителей телефонных разговоров.

Генерирует ABCD-тоны уже известная нам Silver Box.

Тайны маленькой синей коробочки

История настолько невероятная, что можно посочувствовать телефонным компаниям.

Я знакомлюсь с Блю-боксом и его возможностями

Я нахожусь в дорого обставленной гостиной Эла Гилбертсона (настоящее имя изменено), создателя блю-бокса. Гилбертсон держит в руке один из своих блестящих, черных с серебром блю-боксов, указывая на тринадцать маленьких красных кнопок на панели. Он быстро нажимает на кнопки, при этом устройство издает электронный писк различ-

ной частоты. Он пытается объяснить мне, каким образом блю-бокс подчиняет его владельцу всю телефонную сеть планеты, спутники, кабельные сети и прочее. Только и всего.

Что делает блю-бокс?

В случае, если обобщать, он предоставляет пользователю права доступа супер-оператора. Этой кнопкой, захватывается тандем, — Эл нажимает верхнюю кнопку указательным пальцем, — и блю-бокс издает пронзительный писк, а так, — блю-бокс снова пищит, — можно контролировать междугородние коммутационные системы телефонной компании через любой телефонный аппарат, включая телефоны-автоматы. И при этом совершенно анонимно.

Оператор действует из определенного места: телефонная компания знает, где он находится и что делает. А с помощью блю-бокса, после того как захватишь транк, скажем, с бесплатного номера Холидэй Инн, они не знают, кто ты и откуда, они не знают, как ты проскользнул в их сети и подключился к этому бесплатному номеру.

Они даже не подозревают, что вообще происходит что-нибудь незаконное. Кроме того, можно замаскировать свое реальное местонахождение. Можно позвонить соседу через местную линию, потом через Ливерпуль по кабелю и обратно сюда через спутник.

Можно из одного телефона-автомата позвонить на соседний, при этом звонок пройдет по сетям вокруг планеты. И вдобавок ко всему получить обратно свою десятицентовую монету.

Что, и они не могут выследить звонок и начислить за него плату?

В случае, если будешь делать все правильно, то нет. Но ты увидишь, что бесплатные звонки — это не самое интересное. Гораздо более захватывает ощущение власти, которое испытываешь, держа эту крошку в руке. Я наблюдал за людьми, которые впервые приобрели блю-бокс и обнаружили, что могут устанавливать связь с любой точкой на земном шаре. Они совсем не разговаривают с людьми, которым звонят. Просто говорят «здрасьте» и думают, куда бы позвонить еще. У них немного крыша едет.

Он смотрит на аккуратное маленькое устройство в своей ладони и нажимает на кнопки.

Я думаю, все дело в компактном размере моих моделей. Повсюду делают кучу блю-боксов, но мои самые маленькие и навороченные с технической точки зрения. Жаль, что не могу показать тебе модель-прототип, которую мы изготовили для одного синдиката.

Он вздыхает: «У нас был заказ на тысячу пищалок от одного синдиката в Лас-Вегасе».

Они пользуются ими, чтобы делать ставки по телефону, часами занимают телефонные линии, что может влететь в копеечку, если платить, конечно. Сделка была на тысячу блю-боксов по $300 за штуку. До этого мы продавали их в розницу по $1500 за штуку, но, видишь ли, трудно было отказаться от контракта на $300 000. У нас был договор на производство с филиппинцами. Все было готово. Да и вообще, модель, которая была подготовлена для ограниченно серийного производства, запросто помещалась в коробку из-под «Мальборо». У нее были сенсорные кнопки. Выглядела как обычное портативное радио.

На самом деле, в модели был встроен СВ приемник на один канал, чтобы в случае чего, можно было включить радио, и никто бы ни о чем не догадался. Я там все продумал — в устройство был засыпан термит, воспламеняющийся от радио сигнала, с тем, чтобы в случае опасности, блю-бокс превратился бы в пепел за считанные секунды. Он был красивый. Маленькое красивое устройство. Нужно было видеть лица этих мужиков из синдиката, когда они впервые его опробовали. Они вцепились в него мертвой хваткой и повторяли: «Не могу поверить. Не могу поверить». Действительно, трудно поверить, пока сам не попробуешь.

Испытание Блю-бокса: Мы устанавливаем связь

Через два дня около одиннадцати вечера, Фрейзер Люси держит блю-бокс в одной руке и трубку телефона — в другой. Он стоит в телефонной будке неподалеку от закрытого мотеля.

Я стою снаружи.

Фрейзер обожает демонстрировать возможности своего блю-бокса. Еще несколько недель назад, до того, как компания «Пасифик Телефоун» произвела несколько арестов в городе, Фрейзер Люси любил брать блю-бокс с собой на вечеринки. (Его коробочка, как и большинство других, вовсе не синяя. Их стали называть синими либо потому, что первое устройство, конфискованное телефонной компанией, было синего цвета, или для того, чтобы не путать ее с «черными коробочками».)

Черные коробочки — это устройства, обычно представляющие собой набор резисторов и при подключении к домашним телефонам делающие входящие звонки бесплатными.) Он никогда его не подводил: пара «писков» и Фрейзер становился центром внимания в самых хипповых компаниях, показывая разные телефонные фокусы и дозваниваясь по любым номерам. Он даже начал делать заказы производителю в Мексике и стал дилером.

Теперь Фрейзер с осторожностью демонстрирует свой блю-бокс, но ему никогда не надоедает развлекаться с его помощью. «Каждый раз, как в первый раз», — говорит он мне.

Фрейзер опускает десять центов в слот телефона-автомата. Он ждет сигнала готовности и подносит трубку к моему уху. Я слышу гудок. Фрейзер с видом бывалого человека начинает объяснять, что к чему, одновременно действуя. «Сейчас я набираю бесплатный номер. Подойдет любой бесплатный номер. Сегодня это будет *** (он называет известную компанию по прокату автомобилей). Слышишь, звонит? Теперь смотри». — Он прикладывает блю-бокс к микрофону телефонной трубки, так что двенадцать черных кнопок смотрят вверх. Нажимает серебряную кнопку — ту, что сверху — и я слышу пронзительный сигнал. «Это 2600 колебаний в секунду, если быть точным», — говорит Люси. «Теперь слушай скорее». Он протягивает мне трубку. Сигнал вызова прекратился. Линия слегка «кашляет», раздается писк, а после этого ничего, кроме монотонного слабого шума.

«Ну вот мы и на месте, — улыбается Люси, забирает у меня трубку и снова прикладывает к ней блю-бокс. — Мы на тандеме, на междугороднем транке. Теперь можно звонить куда угодно». Сперва он решает проверить связь с Лондоном. Для этого он выбирает специальный телефон-автомат, расположенный рядом с вокзалом Ватерлоо.

Именно этот автомат популярен среди фрикеров, поскольку рядом с ним всегда есть люди, готовые поднять трубку и немного поговорить.

Он нажимает на кнопку, помеченную «KP», на лицевой стороне блю-бокса. «Это Key Pulse. Эта кнопка сообщает тандему, что мы готовы давать ему команды. Для начала наберем KP 182 START, что перебросит нас за океан». Я слышу щелчки. «Пожалуй, соединимся с Европой через спутник. На самом деле кабель быстрее и качество немного выше, но мне нравится соединяться через спутник. Поэтому я просто набираю KP 0 44. Ноль для спутникового соединения, а 44 — код Англии. OK, мы уже там. В Ливерпуле. Теперь я набираю код Лондона, то есть 1, и номер того самого телефона-автомата. Вот, послушай, идет вызов».

Я слышу тихий сигнал вызова в Лондоне. Кто-то снимает трубку.

— Алло, — говорит голос в Лондоне.

— Алло. Кто говорит? — спрашивает Фрейзер.

— Привет. Здесь рядом никого нет. Я просто проходил мимо и снял трубку. Это общественный телефон. На самом деле, здесь рядом звонка никто не ждет.

— Алло. Не вешай трубку. Я звоню из Штатов.

— Да? Ну и зачем? Это же общественный телефон.

— Ну знаешь, просто проверить, что происходит в Лондоне. Как вы там?

— Сейчас пять часов утра. Идет дождь.

— А-а-а. А ты сам-то кто?

Лондонский прохожий оказывается призывником BBC, возвращающимся на базу в Линкольншире с большого похмелья после полутора суток беспробудных возлияний. Они с Фрейзером говорят о дожде и приходят к выводу, что лучше когда светит солнышко. Они прощаются, и Фрейзер вешает трубку. Автомат возвращает его десять центов.

— Ну не здорово ли, — ухмыляется он. Вот так запросто в Лондон.

Фрейзер с любовью сжимает блю-бокс в ладони: «Я же тебе говорил, что это не враки».

— Слушай, если ты не против, я позвоню подружке в Париж. Я всегда звоню ей в это время. Она просто бесится от этого. Теперь я воспользуюсь бесплатным номером *** (называет другую компанию по прокату автомобилей), и мы соединимся с Европой через кабель, 133; 33 — это код Франции, а 1 устанавливает кабельную связь. Ну, поехали. Блин, занято. С кем это она болтает в такой час?

Мимо мотеля проезжает полицейский автомобиль. Автомобиль не останавливается, но Фрейзер заметно нервничает. Мы садимся в его машину и едем в противоположном направлении до бензоколонки «TEXACO», закрытой на ночь. Мы подъезжаем к телефонной будке около пожарного гидранта. Фрейзер забегает в будку и снова пытается дозвониться в Париж. Опять занято.

— Не могу понять, с кем она болтает. Может быть линии заняты. Жалко, что я не умею пока вклиниваться в разговор в Европе с помощью этой штуки.

Фрейзер начинает «шалить», как говорят фрикеры. Он набирает бесплатный номер национального расчетного центра по обслуживанию пластиковых карт и вводит сигналы, соединяющие его со службой точного времени в Сиднее, Австралия. Он звонит в службу погоды в Риме, конечно же, на итальянском. Звонит другу в Бостон и разговаривает о срочно необходимом ему оборудовании. Парижский номер опять занят. Он набирает службу «Dial a Disc» в Лондоне, и мы слушаем песню «Double Barrel» в исполнении Дэвида и Энсил Коллинз, хит номер один

на этой неделе в Лондоне. Звонит другому дилеру и говорит с ним условными фразами. Звонит Джо Энгрессиа, слепому гению в области телефонного фрикинга, и выражает ему свое почтение.

Наконец Фрейзер дозванивается до подружки в Париже.

Они вместе приходят к выводу, что линии, наверное, были заняты и ругают Парижскую телефонную сеть. В два тридцать утра Фрейзер вешает трубку, кладет в карман свои десять центов и уезжает, держа руль в одной руке и свой любимый маленький блю-бокс в другой.

Междугородние звонки могут стоить дешевле, чем вы думаете

— Видишь ли, пару лет назад телефонная компания допустила серьезную ошибку, — объясняет Гилбертсон у себя дома пару дней спустя. — Они толком не подумали и позволили одному техническому журналу опубликовать подлинные частоты, используемые для генерирования мультичастотных тонов. Это была просто теоретическая заметка одного инженера из Белл Телефоун Лабораториз о коммутационной системе, и он мимоходом указал в заметке эти самые частоты. Еще до того, как наткнуться на этот журнал в библиотеке одного технического колледжа, я несколько лет развлекался с этими тонами. Так вот, я бросился прямиком в лабораторию и через двенадцать часов первый работающий блюбокс был готов. Он, конечно же был более громоздкий, чем мои нынешние модели, но работал.

— Информация в этом журнале, который люди из Белл Лэб пишут для других инженеров-телефонистов, абсолютно свободно доступна широкой публике. Ну или по крайней мере была доступна. Можешь попробовать достать экземпляр журнала в библиотеке какого-нибудь технического колледжа. Белл засекретил весь тираж и изъял из обращения, — говорит мне Гилбертсон.

— Но все, поезд ушел. Информация стала достоянием общественности. А раз так, то технология создания своего собственного устройства доступна даже любому двенадцатилетнему пацану, вернее, любому слепому двенадцатилетнему пацану. И изготовить устройство он сможет гораздо быстрее, чем я. Слепые детки всегда этим промышляли.

Они конечно же не в состоянии собрать такой же компактный блю-бокс, как мой, но возможности их модели будут куда как шире.

— В смысле?

— Ладно, слушай. Около двадцати лет назад AT&T приняла многомиллионное решение перевести все свои междугородние линии связи

на управление двенадцатью комбинациями двенадцати же электронных тонов. Именно эти тоны ты слышишь иногда при междугородней связи.

— Они не стали ничего особо усложнять — тон для каждой цифры представляет собой комбинацию двух отдельных тонов. Например, 1300 колебаний в секунду плюс 900 колебаний в секунду при одновременном воспроизведении дадут тон для цифры 5. Так вот, эти фрикеры стали доставать себе электроорганы. В общем, пойдет даже самый дешевый домашний электроорган. И поскольку частоты стали доступными всем — один слепой фрикер даже занес их в «говорящую» книгу для слепых — им просто осталось подобрать на органе музыкальные ноты, соответствующие телефонным тонам. Потом они записывают их на магнитофон. Например, чтобы получить тон, соответствующий цифре 1 по стандартам Ма Белл, надо просто одновременно нажать на органе ноты F-5 и A-5 (900 и 700 колебаний в секунду соответственно). Для цифры 2 — F-5 и C-6 (1100 и 700 Гц). Фрикеры составили полный список тонов и соответствующих им нот, так что теперь не ошибешься.

Он показывает мне список всех остальных цифр и комбинаций органных клавиш для их генерирования.

— На самом деле, записывать тоны на пленку надо на скорости 3,75 дюйма в секунду, а воспроизводить — со скоростью 7,5 дюймов в секунду. Тогда все получится правильно, — добавляет он.

— Хорошо, а как ввести эти тоны в сеть, после того, как их запишешь?

— Ну, они берут свой орган и магнитофон и начинают набивать на органе целые комбинации номеров, включая междугородние коды, команды маршрутизации, сигналы «КР» и «Старт». Или если у них нет органа, кто-нибудь из других фрикеров дает им кассету со всеми тонами, где голос сообщает «Номер один», после чего звучит тон «Номер два». Так что при наличии двух магнитофонов можно комбинировать любые номера, переключаясь с одного магнитофона на другой. Любой придурок с дешевым магнитофоном может при желании звонить на халяву.

— Ты хочешь сказать, что нужно просто поднести магнитофон к телефонной трубке, включить запись, и телефон подумает, что тоны сгенерированы им самим?

— Именно. Пока частоты находятся в пределах 30 колебаний в секунду, телефон считает, что слышит свой собственный голос. Дедушкой фрикинга был один слепой парень с абсолютным слухом, Джо Энгрессиа, который просто свистел в трубку. Телефонист, конечно, мог отличить его свист от электронного, а коммутационное оборудование — нет.

Чем больше телефонная компания, тем меньше в ней живых телефонистов и тем уязвимее для фрикинга она становится.

Пояснение для тех, кто ничего не понял

— Но погоди, — останавливаю я Гилбертсона. В случае, если можно так здорово подражать оборудованию, то почему телефонная компания не выставляет счета за эти звонки?

— О'кей. Вот тут-то и появляется на сцене сигнал 2600 Гц. Пожалуй, лучше я начну с самого начала.

Сперва он описывает мне устройство телефонной сети страны как огромной паутины транков, исходящих от одних коммутационных узлов к другим. Коммутационный узел состоит из тысяч междугородних тандемов постоянно свистящих или передающих тоны другим удаленным коммутационным узлам.

Понятие тандема является ключевым для всей системы. Он представляет собой линию с подключенными к ней реле, которая может посылать сигналы любому другому тандему на любом коммутационном узле страны. Он может делать это напрямую или создавая обходной маршрут через несколько других тандемов, если все прямые маршруты заняты.

Например, если вы хотите позвонить из Нью-Йорка в Лос-Анджелес при большой загруженности трафиком линий между двумя городами, ваш нью-йоркский тандем автоматически попробует установить связь через другой наиболее оптимальный маршрут, по которому ваш вызов пойдет, скажем, в Новый Орлеан, затем в Сан-Франциско или обратно в Новый Орлеан, назад в Атланту и оттуда через Альбукерке в Лос-Анджелес.

Когда тандем не используется и ждет, пока кто-нибудь позвонит по межгороду, он свистит. Одна сторона тандема, обращенная к твоему домашнему телефону, свистит сигнал частотой 2600 колебаний в секунду по всем линиям, обслуживаемым твоей подстанцией, и тем самым сообщает о своей доступности на тот случай, если кто-нибудь захочет набрать междугородний номер.

Другая сторона тандема свистит 2600 колебаний в секунду в междугородние транки, информируя всю остальную телефонную сеть, что он в настоящий момент не использует данный транк для передачи разговора.

При наборе междугороднего номера ты первым делом соединяешься с тандемом. По нему посылается набранный тобой номер. Эта исходящая сторона тандема перестает свистеть 2600 в транк. После того, как тандем перестал подавать сигнал 2600 в транк, говорят, что произошел «захват транка», и по нему теперь возможна передача набранного тобой номера — преобразованного в мультичастотные тоны — на тандем в зоне набранного междугороднего кода.

Так вот когда обладатель блю-бокса хочет позвонить из Нового Орлеана в Нью-Йорк, он первым делом набирает бесплатный номер компании, головной офис которой находится в Лос-Анджелесе.

Посылающая сторона новоорлеанского тандема перестает подавать 2600 в транк, идущий до Лос-Анджелеса, происходит захват транка.

Новоорлеанский тандем начинает посылать тоновые сигналы в тандем в Лос-Анджелесе, который до этого подавал сигнал «свободен».

Принимающая сторона лос-анджелесского тандема перестает свистеть 2600 Гц, принимает тоновые сигналы номера и начинает набор бесплатного номера в Лос-Анджелесе. Одновременно тарификационное оборудование в Новом Орлеане делает запись о том, что был произведен звонок из Нового Орлеана в Лос-Анджелес по бесплатному номеру, и присваивает звонку кодовый номер. До этого момента все происходит как обычно.

Но тут фрикер прижимает свой блю-бокс к трубке и нажимает кнопку, посылая сигнал 2600 с новоорлеанского тандема в тандем Лос-Анджелеса. Лос-анджелесский тандем видит, что через линию снова идет сигнал 2600 Гц и думает, что абонент в Новом Орлеане повесил трубку, поскольку транк подает сигнал «свободен». Тандем в Лос-Анджелесе немедленно прерывает вызов местного абонента. Но как только фрикер отпускает кнопку, тандем в Лос-Анджелесе начинает думать, что транк снова занят, поскольку сигнал 2600 пропал, и ожидает приема новых цифровых тонов — чтобы узнать, по какому номеру звонить.

В итоге, пользователь блю-бокса из Нового Орлеана может теперь управлять тандемом в Лос-Анджелесе, как захочет.

Фрикер набирает затем десять цифр номера в Нью-Йорке и тем самым приказывает лос-анджелесскому тандему перевести звонок в Нью-Йорк.

Что он и делает. Когда вызываемый абонент в Нью-Йорке поднимет трубку, сторона новоорлеанского тандема, обращенная к звонящему, прекращает подавать в линию 2600 и начинает передавать его голос в Нью-Йорк через лос-анджелесский тандем. На тарификационной пленке делается отметка, что был набран бесплатный номер в Лос-Анджелесе.

Когда разговор с Нью-Йорком окончится, соответствующая запись появится и на пленке.

В три часа на следующее утро, когда главный тарификационный компьютер телефонной компании начнет производить учет междугородних звонков за предыдущие сутки, выяснится, что с домашнего номера в Новом Орлеане был произведен звонок по бесплатному номеру в Лос-Анджелесе, ну и, разумеется, компьютер не включает звонки по бесплатным (начинающимся на 1–800) номерам в месячный счет за услуги связи.

Единственное, что они могут доказать, это то, что ты позвонил по бесплатному номеру, — завершает свой рассказ Гилбертсон.

— Конечно, если ты по глупости в течение двух часов разговаривал с бесплатным абонентом, и телефонная компания установила специальный компьютер для отслеживания подобных вещей, у них может возникнуть резонный вопрос, почему ты два часа разговаривал по бесплатному номеру со службой набора рекрутов в армию, если у тебя «белый билет».

Но если проделывать это с телефона-автомата, они, конечно, обнаружат нечто интересное на следующее утро, но тебя уже и след простынет. При использовании телефонов-автоматов безопасность практически стопроцентная.

— А как же насчет недавней серии арестов людей с блю-боксами по всей стране — в Нью-Йорке, Кливленде и других городах? — спрашиваю я. — Что ж они так легко попались?

— Насколько я знаю, они допустили одну грубую ошибку: они захватывали транки при помощи кода города и номера 555–1212 вместо бесплатного номера. Когда человек набирает 555, это легко определить, поскольку при наборе такого номера делается соответствующая запись, и компьютер при выставлении тебе счета за двухчасовой звонок в Огайо автоматически сообщает эту информацию агентам по безопасности.

Тот, кто продал этим ребятам блю-боксы, толком не объяснил, как ими пользоваться, что, конечно, крайне безответственно. А те дурачки тоже хороши: все время звонили с домашнего номера.

Интересно то, что после этих арестов блю-боксы стали еще большими партиями завозиться в страну. Ма Белл в беде.

— А что, если фрикер будет постоянно пользоваться телефонами-автоматами и бесплатными номерами, телефонная компания не сможет ему ничего сделать?

— Нет, если они, конечно, не заменят по всей стране систему междугородней связи, на что у них уйдет несколько миллиардов долларов и двадцать лет. Сейчас они ни черта не могут поделать. Они в полной заднице.

Капитан Кранч демонстрирует свое знаменитое устройство

В США существует подпольная телефонная сеть. Гилбертсон обнаружил это в тот же день, года известия о его подвигах появились в прессе. В тот вечер его телефон надрывался от звонков.

Фрикеры из Сиэтла, Флориды, Нью-Йорка, Сан-Хосе и Лос-Анджелеса звонили ему и сообщали о фрикерском подполье. Один из них просто сказал:

— Повесь трубку и набери этот номер.

Когда Гилбертсон набрал номер, он очутился на сеансе конференц-связи с десятком фрикеров. Связь была организована через коммутационный узел в Британской Колумбии.

Они представились телефонными фрикерами, рассказали ему о своих блю-боксах, которые, кстати, они называли «мультичастотниками», и прочих фрикерских штучках. Они посвятили его во многие свои тайны, посчитав факт преследования со стороны телефонной компании хорошим доказательством его благонадежности.

И, как вспоминает Гилбертсон, он был буквально ошеломлен осведомленностью фрикеров в технических вопросах.

Я спросил его, как выйти на контакт с фрикерами. Он порылся в ящике со старыми электронными схемами и достал листок с десятком номеров в разных регионах страны.

— Это центры, — говорит он мне. Рядом с номерами он записывает имена или прозвища типа Капитан Кранч, Доктор Нет, Фрэнк Карсон, Марти Фримэн, Питер Перпендикулярный Прыщ, Алефноль и Чеширский Кот. Рядом с именами слепых фрикеров он ставит галочки. Всего пять галочек.

Я спрашиваю его о Капитане Кранче.

Он, наверное, самый легендарный фрикер. Он выбрал себе это прозвище в честь знаменитого свистка из упаковок Капитан Кранч. (Несколько лет назад, объясняет Гилбертсон, производители овсяной каши марки Капитан Кранч стали класть игрушечный свисток в каждую упаковку для привлечения покупателей. И какой-то фрикер случайно

обнаружил, что этот свисток выдает звук частотой 2600 Гц. Когда человек, называющий себя Капитаном Кранчем, был переведен со своим батальоном ВВС на службу в Англию, он помогал своим товарищам звонить бесплатно при помощи этого самого свистка.)

— Капитан Кранч это один из самых заслуженных фрикеров, — говорит Гилбертсон. — В сущности, он инженер, который развлекался с телефоном и однажды попался на этом, но остановиться уже не мог.

Сейчас он разъезжает по стране на фургоне Фольксваген, напичканном целым коммутационным узлом и навороченным компьютеризированным мультичастотным генератором сзади. Он обычно подъезжает к телефонной будке на каком-нибудь безлюдном шоссе, протягивает кабель от своего фургона и часами, а иногда и сутками, напролет развлекается с телефонной сетью.

Вернувшись в мотель, я набрал номер Капитана Кранча, который мне дал Гилбертсон, и спросил Г*** Т***, то есть его реальное имя или, по крайней мере, имя, которое он использует, когда не занимается фрикингом.

Когда Г*** Т*** подошел к телефону, я сказал ему, что пишу статью в журнал «Эсквайр» о телефонных фрикерах. Он разозлился.

— Я этим больше не занимаюсь. А если и занимаюсь, то только по одной причине. Только для того, чтобы больше узнать о системе. Телефонная компания — это Система. Компьютер — это тоже Система. Понимаешь? В случае, если я что-то и делаю, то только для пополнения знаний о системе. Компьютеры, системы — это моя стихия. Телефонная компания на самом деле не что иное, как компьютер.

В голосе Капитана начинает звучать сдерживаемое возбуждение, когда речь заходит о системах. Он начинает отчетливо произносить каждый слог.

— Ма Белл — это та система, которую я хочу исследовать. Это очень изящная система, но она в дерьме. Это ужасно, потому что Ма Белл такая изящная система, но она в дерьме. Я узнал об этом от пары слепых ребят, которые просили меня изготовить устройство. Необычное устройство. Они сказали, что с его помощью можно звонить бесплатно. Это меня не интересовало. Но когда эти самые слепые пацаны сказали мне, что с его помощью также можно прозваниваться на компьютеры, мои глаза загорелись. Я хотел побольше узнать о компьютерах. Я хотел узнать все о компьютерах Ма Белл. Поэтому я собрал это устройство, но собрал его неправильно, и Ма Белл вышла на мой след. Ма Белл имеет возможность отслеживать подобные штучки. Поэтому я больше не пользуюсь такими устройствами. Никогда. Разве что для исследовательских целей. — Он на время прерывается.

— Так ты, значит, хочешь написать статью. Ты платишь за этот звонок? Повесь трубку и набери вот этот номер. — Он говорит мне номер с междугородним кодом за тысячи миль от своего местонахождения. Я набираю номер.

— Привет еще раз. Это Капитан Кранч. Ты говоришь со мной через бесплатную петлю в Портленде, Орегон. Ты знаешь, что такое бесплатная петля? Я тебе расскажу.

Он объясняет мне, что почти на каждой телефонной подстанции есть тестовые номера, которые позволяют проверять качество связи с другими подстанциями. Большинство таких номеров отличаются друг от друга на единицу, к примеру 302 956-0041 и 302 9560042. Так вот какие-то фрикеры обнаружили, что если двое из разных концов страны одновременно позвонят по двум таким номерам, то они смогут разговаривать, как если бы позвонили друг другу. И, конечно же, бесплатно для обоих.

— Сейчас наши голоса закольцовываются через коммутатор в Канаде, — говорит Капитан.

— Мой голос идет туда и обратно к тебе. И абсолютно бесплатно. Фрикеры и я составили длинный список таких последовательных номеров. Ты удивишься, если увидишь список. Я бы тебе его показал, но не могу. Я завязал. Я не собираюсь развлекаться с Ма Белл. Мне виднее. В случае, если я что-нибудь и предпринимаю, то исключительно в познавательных целях. Тут можно многому научиться. Ты когда-нибудь слышал об одновременной стыковке восьми тандемов? Тебе знаком звук стыковки и расстыковки тандемов? Дай мне твой номер. О'кей. Повесь трубку и подожди немного.

Через минуту телефон зазвонил, и я услышал голос Капитана Кранча на том конце провода. Его голос звучал еще более возбужденно.

— Я хотел продемонстрировать тебе, что значит стыковать тандемы. (Когда Капитан произносит слово «стыковать», кажется, что он облизывает губы.)

— Как тебе нравится соединение, через которое мы сейчас говорим? — спрашивает меня Капитан. — Это просто тандем. Сейчас я покажу тебе, что значит стыковать тандемы. Надо несколько раз пересечь страну, а затем соединиться с Москвой.

— Слушай, — продолжает Капитан Кранч. — Слушай. Я тут занял линию на местной подстанции и хочу, чтобы ты услышал, как я буду стыковать тандемы. Слушай. У тебя крыша поедет.

Сперва я слышу пулеметную очередь тональных сигналов, похожих на звуки флейты, затем пауза, потом еще серия тонов, еще и еще. После каждой серии звучит щелчок.

— Мы сейчас состыковали четыре тандема, — говорит Капитан Кранч, как бы издалека.

— Сейчас состыковано четыре тандема. Ты знаешь, что это значит? Это значит, что мой голос четыре раза пересекает страну туда и обратно, прежде чем дойти до тебя. В свое время я стыковал по двадцать тандемов кряду. Сейчас, как я и говорил, я прозвонюсь в Москву.

Звучит новая серия сигналов, короткая пауза, затем сигнал вызова.

— Алло, — говорит удаленный голос.

— Алло. Это американское посольство в Москве?

— Да, сэр. А кто звонит? — говорит голос.

— Да-а-а. Это проверка связи с Нью-Йорком. Мы звоним, чтобы проверить, какие у вас линии. Все там, в Москве, в порядке?

— В порядке?

— Ну да. Как вы там поживаете?

— Да вроде бы все нормально.

— О'кей. Спасибо.

Оба абонента повесили трубку, и в линии некоторое время еще слышались постепенно затухающие гудки.

Заметно, что Капитан доволен.

— Ну теперь-то ты мне веришь? Ты знаешь, что я не против сделать? Я хочу позвонить твоему редактору из «Эсквайра» и продемонстрировать ему, что значит стыковать тандемы. У него крыша поедет от моего шоу. Какой у него телефон?

Я спрашиваю у Капитана, при помощи какого устройства он все это проделывает. Капитану нравится вопрос.

— А ты заметил, что это нечто особенное, так ведь? Десять импульсов в секунду. Это быстрее, чем оборудование АТС. Поверь мне, это устройство — самое знаменитое в стране. Другого такого нет. Поверь мне.

— Да, я слышал о нем. Мне какие-то фрикеры рассказали.

— Они ссылались на мое устройство? Как они его описывали? Просто любопытно, не говорили ли они, что это навороченное устройство с компьютерным управлением, с акустическим соединением для приема сигналов и многоканальным коммутационным узлом? Не говорили ли они, что погрешность частоты не превышает 0,05%, а погрешность амплитудных колебаний — 0,01 децибел?

— Импульсы, которые ты слышал, совершенны. Они быстрее АТСных. Это из-за высококачественных усилителей. Эти усилители созданы для сверхстабильного усиления, сверхнизкого искажения сигнала и правильной передачи частот. Они не сказали тебе, что прибор может работать при температуре от -55°С до +125°С?

Я признаю, что ничего из этого я не знал.

— Я эту штуку сам построил, — продолжает Капитан. — В случае, если бы ты сам захотел собрать нечто подобное и покупал бы детали у оптовиков, тебе потребовалось бы по меньшей мере $1500. А я просто одно время работал на компанию по производству полупроводников, и мне это ни копейки не стоило. Ты понимаешь, что я хочу сказать? Они рассказывали тебе, как я однажды произвел телефонный звонок вокруг света? Я тебе расскажу. Я набрал Токио, оттуда соединился с Индией, из Индии — с Грецией, из Греции — с Преторией, из Южной Африки — с Южной Америкой, оттуда — с Лондоном, лондонский телефонист соединил меня с нью-йоркским телефонистом, из Нью-Йорка я позвонил оператору в Калифорнии, который набрал номер телефона, расположенного возле меня.

Естественно, мне приходилось кричать в трубку, чтобы услышать себя. И эхо было сильным. Фантастика.

Задержка составляла двадцать секунд, но я мог слышать свой собственный голос и разговаривать с собой.

— Ты хочешь сказать, что говорил в одну трубку, твой голос облетал весь мир и возвращался к тебе из другой трубки? — спросил я Капитана. В этом мне виделось нечто смутно автоэротичное, только в сложноэлектронной форме.

— Именно, — сказал Капитан. Я также посылал свой голос вокруг света в одном направлении, с востока на запад, и одновременно в обратном направлении — с запада на восток, при этом оба сигнала проходили через кабель в первом случае и через спутник — во втором. Сигналы возвращались ко мне одновременно. Чудеса, с ума сойти можно.

— Ты хочешь сказать, что ты сидишь с двумя трубками и разговариваешь сам с собой вокруг света? — спросил я недоверчиво.

— Да. Именно так. Я соединяю обе линии, сижу и разговариваю.

— Ну и что же ты говоришь в трубку сам себе?

— Ну, знаешь. Алло, проверка связи, раз, два, три, — говорит он приглушенно. — Алло, проверка связи, раз, два, три, — отвечает он себе громко. — Алло, проверка связи, раз, два, три, — повторяет он снова приглушенно. — Алло, проверка связи, раз, два, три, — повторяет он громко. — Иногда я говорю просто: Алло, алло, алло, алло, алло, — смеется он.

Почему капитан Кранч больше не прослушивает телефонные линии

С помощью служебных кодов телефонных компаний фрикеры нашли простой способ прослушивать телефонные разговоры. Операторы телефонной станции сидят перед панелью с контрольными штекерами.

Это устройство позволяет им подключиться к разговору в чрезвычайном случае и проверить состояние линии. Фрикеры научились при помощи особых сигналов связываться с таким оператором. Они представляются телефонистом из другой местности, проверяющим междугородние транки. Как только оператор переключает фрикера на тестовый транк, фрикер незаметно проскальзывает на любую из десятков тысяч линий на данной подстанции, при этом ни оператор, ни, разумеется, пользователи сети не знают, что их разговор прослушивается.

Под конец нашей часовой беседы я спрашиваю у Капитана, не пробовал ли он прослушивать телефоны.

— Нет. Этим я не занимаюсь. По-моему, это некрасиво, — говорит он убежденно. — Я, конечно, имею подобную возможность, но никогда ею не пользовался. Ну разве что однажды, только однажды.

Эта девчонка, Линда, я просто хотел выяснить: ну ты понимаешь. Я хотел позвонить ей и назначить свидание. Мы с ней уже виделись на предыдущей неделе, и мне показалось, что я ей пришелся по вкусу. Так вот, я набираю ее номер, а там занято. Я снова набираю — опять занято. Я только недавно узнал этот способ незаметно подключаться к телефонным линиям, и я говорю себе: «Гммм. Почему бы не проверить этот способ? Она, наверное, удивится, если мой голос вдруг окажется у нее в трубке. В любом случае это ее впечатлит». Ну, я так и сделал. Я стал подавать сигналы в линию. Моя пищалка позволяет обойтись без оператора, если подавать сигналы непосредственно в трубку.

Я подключился к линии, а она болтала с другим парнем. Сладенько так болтала. Мне стало так противно, что я не проронил ни звука. Я дождался, пока они окончат флиртовать и повесят трубку. Потом я сразу же набрал ее номер и сказал: «Линда, между нами все кончено». Она, конечно, не могла понять, что же на самом деле произошло.

Но это был единственный случай. Я надеялся удивить ее, произвести впечатление. Это были мои единственные намерения, а вылилось это в совсем другое. С тех пор я никогда не прослушиваю телефоны.

Спустя некоторое время мой первый разговор с Капитаном подходит к концу.

— Послушай, — говорит он, немного приободрясь. Когда я повешу трубку, ты услышишь звук расстыковки тандемов. Слой за слоем, пока ничего не останется. Щелк, щелк, щелк, — завершает он, плавно переходя на шепот.

Он вешает трубку. Телефон неожиданно начинают сотрясать спазмы: щелк, щелк, щелк: и навороченная схема соединения растворяется, как улыбка Чеширского кота.

Мультичастотное буги

Следующим телефонным номером из списка предоставленного мне изобретателем блю-бокса был номер в городе Мемфис. Номер Джо Энгрессиа, первого и, пожалуй, самого знающего из слепых фрикеров.

Три года назад об Энгрессиа в течение девяти дней шумели все газеты и журналы по всей Америке — его поймали, когда он высвистывал бесплатные междугородние подключения для сокурсников в Университете Южной Флориды. У Энгрессиа врожденный совершенный слух, он мог высвистывать сигналы телефонной станции лучше, чем сама станция.

Энгрессиа мог бы так и продолжать высвистывать для нескольких друзей, если бы телефонная компания не пожелала придать делу огласку. Его предупредили в колледже и подвергли дисциплинарному наказанию. После сообщений СМИ о талантах Энгрессиа, парню стали поступать странные звонки. Звонили какие-то пацаны из Лос-Анджелеса, которые могли выкидывать разные штуки с сетями «General Telephone and Electronics».

Звонили группы практически слепых подростков из Калифорнии, которые ставили увлекательные эксперименты со свистками «Капитан Кранч» и тестовыми петлями. Звонили из Сиэтла, Кембриджа, штат Массачусетс, Нью-Йорка и из других точек страны. Некоторые из зво-

нивших фрикеров уже имели магнитные записи тонов и мультичастотные генераторы. Некоторые с удивлением узнавали о существовании единомышленников в других уголках страны.

Публичное представление Энгрессиа стало катализатором для объединения доселе разрозненных центров фрикинга. Они все связывались с Энгрессиа. Делились с ним своими идеями, рассказывали о своих проектах, задавали вопросы. А он сообщал звонящим координаты других фрикерских групп и объединений, называл телефоны, и примерно через год сам собой сформировался единый всеамериканский фрикерский андеграунд.

Сейчас Джо Энгрессиа только двадцать два года, но среди фрикеров он считается «стариком», уважаемым так же, как Александр Грэм Белл среди телефонистов. Ему больше почти не приходится звонить самому. Фрикеры постоянно звонят ему и сообщают о своих новых находках и изобретениях. Каждую ночь он сидит, как слепой паук, в своей крохотной квартирке и принимает сигналы со всех концов своей паутины. Он гордится, что ему так часто звонят.

Но когда я застал его тем вечером в его квартире в Мемфисе, Джо Энгрессиа был одинок и подавлен.

— Боже, как я рад, что хоть кто-нибудь позвонил. Я не знаю почему, но сегодня на удивление мало звонков. Этот козел сегодня снова нажрался и полез ко мне с грязными предложениями. Я уже устал повторять ему, что мы с ним по этому вопросу никогда не договоримся, если ты, кончено, понимаешь, о чем я. Но он никак не въезжает. Он напивается все сильнее, и я не знаю, что ему далее в голову взбредет. Просто я здесь совсем один, только что переехал в Мемфис, впервые живу самостоятельно, и мне очень не хотелось бы, чтобы все это разрушилось. Но я с ним спать не собираюсь. Просто секс меня не очень волнует, и даже хотя я и не могу видеть его, я знаю, что он урод.

— Ты слышал? Это он стучит бутылкой в стену. Милашка. Ладно, ну его на фиг. Ты пишешь статью о фрикерах? Тогда слушай. Это Мультичастотное буги.

Разумеется, в линии слышится хриплая версия известного буги «Muskrat Ramble», каждая нота которого представлена в виде тонального сигнала. Музыка останавливается. В телефонной трубке слышится громоподобный голос: «Вопрос в том, может ли слепой собрать усилитель?».

Грохот прекращается. Его сменяет высокий голос, похожий на голос телефонистки: «Это телефонная компания Southern Braile Tel. & Tel. Мы готовы принять ваш звонок».

Потом звучит последовательность мультичастотных сигналов, мягкий щелчок и густой голос: «В случае, если вам требуется помощь по дому, обратитесь в службу приходящих домработниц. Точное время в Гонолулу 16:32».

Джо снова говорит своим нормальным голосом: «Мы смотрим друг другу в глаза? Си, си, говорит слепой мексиканец. Гммм. Ты хочешь узнать погоду в Токио?».

Этот фрикерский водевиль на время отвлекает Джо от мыслей о его мучителе.

— Ты можешь спросить, почему я в Мемфисе и почему я должен зависеть от этого педика.

Просто я впервые могу жить сам по себе и звонить сам по себе. Мне запретили доступ во все телефонные компании дома во Флориде, они слишком хорошо меня знают, а студенты в Университете не любили меня за то, что я постоянно висел на телефоне-автомате в общежитии, и смеялись над моей толстой задницей, которая у меня на самом деле толстая, но мне неприятно постоянно об этом слышать. А если я не могу заниматься фрикингом, я просто погибаю. Три четверти прожитого мной времени было посвящено фрикингу.

— Я переехал в Мемфис, потому что хотел жить самостоятельной жизнью и потому что здесь находятся телефонные узлы интересных систем, и они меня пока не знают, так что я могу «путешествовать» в свое удовольствие.

«Путешествие» начинается, по объяснению Джо, со звонка в машинный зал центральной АТС. Он вежливо говорит телефонисту, что он слепой студент, интересующийся телефонными системами, и просит совершить экскурсию по АТС. Во время такой экскурсии Джо обожает трогать руками реле, гладить коммутаторы и прочие устройства.

Поэтому, когда Джо начинает «фрикать», он чувствует и слышит переключение каждого реле, каждой линии и тандема. Вся система компании Белл пляшет под его дудку.

Всего месяц назад Джо снял в банке все свои сбережения и уехал из дома, невзирая на протесты матери. «Я практически бежал из дома», — говорит он. Джо снял небольшую квартиру на Юнион Авеню и начал совершать «путешествия». Он ехал автобусом за сотню миль к югу в штат Миссисипи, чтобы лично ознакомиться с допотопным оборудованием компании Белл, все еще используемым в некоторых регионах. Он ехал на автобусе за триста миль в Шарлотт, Северная Каролина, чтобы взглянуть на новейшее экспериментальное оборудование. Он нанимал такси и ехал

за двенадцать миль в пригород, чтобы совершить «экскурсию» по помещениям одной маленькой телефонной компании, которая имела интересную схему коммутации. Это было лучшее время его жизни, говорит Джо, максимум свободы и удовольствия, которые он когда-нибудь имел.

В течение того месяца он очень редко занимался междугородним фрикингом со своего собственного телефона. Как он говорит, он хотел получить работу в телефонной компании и потому держался в стороне от незаконной деятельности.

— Меня устроила бы любая работа, даже должность самого младшего оператора. Да они, по всей видимости, и не предложили бы мне ничего большего из-за моей слепоты, хотя я и знаю намного больше, чем многие зрячие телефонисты. Но я не в обиде. Я хочу работать на Ма Белл. Я не испытываю по отношению к этой компании такой ненависти, как Гилбертсон и некоторые другие фрикеры. Я не ставлю задачей навредить Ма Белл. Я получаю удовольствие исключительно от процесса познания. В случае, если ты знаешь систему так же близко, как я, ты начинаешь видеть в ней некую красу. Но я не в курсе, насколько хорошо они осведомлены обо мне. Я очень тонко чувствую состояние линии, по которой разговариваю, и у меня есть подозрение, что за мной наблюдают в последнее время. Периодически мне приходится звонить телефонистам (что не совсем законно).

Однажды я наелся ЛСД и у меня начались слуховые глюки, как будто я попался в ловушку, и меня бомбили какие-то самолеты, и неожиданно мне надо было при помощи фрикинга выбираться оттуда. Почему-то мне было нужно позвонить в Канзас-Сити.

Поступает предупреждение

В этот момент — в час ночи по местному времени — громкий стук в дверь гостиничного номера прерывает нашу беседу. В двери стоит охранник в униформе и сообщает, что пока я разговаривал по телефону, на мое имя поступил экстренный вызов, и администратор попросил позвать меня.

Через две секунды после того, как я прощаюсь с Джо и вешаю трубку, раздается телефонный звонок.

— С кем ты разговаривал? — интересуется взволнованный голос Капитана Кранча. Я звоню, чтобы предупредить тебя кое о чем. Будь осторожен. Я не хочу, чтобы информация, которую ты получаешь, поступила в распоряжение радикального андеграунда. Я не хочу, чтобы она попала не в те руки. Что если я скажу тебе, что три фрикера при желании могут парализовать телефонную сеть всей страны? Всей страны! Я знаю, как это

можно сделать. Но я не скажу. Один мой приятель уже пробовал парализовать транки между Сиэтлом и Нью-Йорком при помощи компьютеризированного генератора мультичастотных тонов. Но есть и более простые способы сделать это.

— Всего три человека? — спрашиваю я. — Разве это возможно?

— Ты когда-нибудь слышал о защитной частоте междугородних линий? Ты знаешь что-нибудь о стыковании тандемов при помощи 17 и 2600? В случае, если нет, то я советую тебе узнать про это. Я тебе сам рассказывать не буду. Но что бы ты ни делал, не дай бог, если это попадет в лапы радикального андеграунда.

Позже Гилбертсон, изобретатель блю-бокса, признался, что хотя он всегда и сохранял скептическое отношение к рассказам Капитана о возможности саботировать работу телефонной сети при помощи занятия транков, недавно ему продемонстрировали нечто, что разубедило его в тщетности рассказов Капитана. «Мне кажется, что для этого понадобится больше, чем три аппарата, подобных аппарату Капитана Кранча». Но даже хотя рассказам Капитана верится с трудом, он все-таки зачастую знает, о чем говорит.

— Ты знаешь, — продолжает Капитан увещевающим тоном, — ты знаешь, начинающие фрикеры постоянно звонят в Москву. Представь, если бы все звонили в Москву. Я не принадлежу к ультраправым. Но мне дорога моя жизнь. Мне не хотелось бы, чтобы коммунисты прилетели сюда и сбросили бомбу мне на голову. Вот почему я советую тебе распространять информацию с осторожностью.

Капитан неожиданно переключается на поношение фрикеров, ненавидящих телефонные компании.

— Они не могут понять, что Ма Белл знает все об их штучках. Ма Белл знает. Послушай, мне что-то не нравится. Кажется, к нашей линии только что кто-то подключился. Я не параноик, но такие вещи всегда замечаю. Ну даже если это так и есть, они знают, что я знаю, что они знают, что у меня есть устройство для стирания магнитных записей. Я совершенно чист. — Капитан делает паузу, очевидно, разрываясь между желанием показать телефонной компании, что не делает ничего противозаконного, и стремлением продемонстрировать мне свою удаль.

— Ма Белл знает на что я способен. А способен я на многое. Я могу определять обратную связь, переключение тандемов, все, что происходит на линии. У меня хороший слух выработался. Ты понимаешь, о чем я? Мои уши равноценны оборудованию за $20 000. Я могу слышать то, что они не могут со всем своим оборудованием. У меня были проблемы с

работой. Я терял работу. Но я хочу показать Ма Белл, насколько я хорош. Я не хочу вредить компании, я хочу работать на нее. Я хочу работать ей на благо. Я хочу помочь ей избавиться от недостатков и стать совершенной. На данный момент это моя главная цель в жизни. — Капитан заканчивает свои увещевания и говорит, что больше не может разговаривать. — На этот вечер у меня тут одно мероприятие запланировано, — объясняет он и вешает трубку.

Перед сном я перезваниваю Джо Энгрессиа. Он сообщает, что его мучитель наконец-то заснул.

— Он конечно, не в ж... надрался, но все равно порядочно. Я назначаю встречу с Джо через два дня в Мемфисе.

Телефонный звонок фрикера все улаживает

На следующий день я посещаю встречу четырех фрикеров в *** (один из калифорнийских пригородов). Встреча происходит в комфортабельном доме в несколько этажей. На кухонном столе свалены портативные магнитофоны, кассеты с записями мультичастотных тонов, телефонные провода, принадлежащие присутствующим фрикерам. Рядом лежит внушительных размеров блю-бокс с тринадцатью кнопками для активации разных тонов.

Родители слепого фрикера — хозяина квартиры, Ральфа, сидят в соседней комнате с другими детьми. Они не вполне в курсе, чем Ральф с друзьями занимаются и законно ли это, но их сын слеп, и родители рады любому его хобби.

Группа разрабатывает проект по проведению исторической конференции «2111», восстанавливает некоторые бесплатные «петли» и пытается разобраться в новых уловках телефонистов против фрикеров. Вскоре мне удалось увидеть Рэнди в деле. Рэнди бледен, мягкотел, носит мешковатые штаны и неглаженную белую футболку, периодически вытягивает шею, как черепаха. Его глаза постоянно в движении, немного косят, а лоб — в прыщах. Ему всего шестнадцать.

Но когда Рэнди говорит в трубку, его голос становится столь поразительно солидным, что приходится снова взглянуть на него, дабы убедиться, что голос действительно принадлежит нескладному подростку Рэнди. Представьте голос матерого нефтяника-буровика или просмоленного сорокалетнего Мальборо-мэна. Представьте голос удачливого биржевика, рассказывающего, как он сбивает Доу-Джонс на 30 процентов. Теперь представьте голос, который звучал бы одновременно и как Стивен Фетчит. Это голос шестнадцатилетнего Рэнди.

Он разговаривает с телефонистом из Детройта. Телефонная компания в Детройте без видимой причины закрыла две бесплатные петли, хотя они, конечно, могли обнаружить активную деятельность фрикеров. Рэнди рассказывает оператору, как разблокировать петлю и снова сделать ее бесплатной:

— Как жизнь, дружище? Ага. Я за пультом здесь в Тулса, Оклахома, мы пытались проверить ваши петли, так они постоянно заняты с обоих концов... Ну да, там постоянно «BY». Как ты думаешь, на них карты кинуть можно? У тебя 08 в номерной группе есть? А-а-а, ну в принципе все нормально, у нас такое уже было, надо сеть проверить. Вот, слушай: твой бокс 05, вертикальная группа 03, горизонтальная — 5, вертикальный файл 3. Да, мы подождем... О'кей, нашел? Отлично. Хорошо, мы хотели бы расчистить «бизю». Да. Тебе только надо найти ключ на крепежной панели. Это в твоем транковом боксе. О'кей? Теперь переставь ключ из NOR в LCT. Не знаю почему, но у нас с этим проблемы. О'кей. Спасибо, дружище. Пока.

Рэнди кладет трубку, сообщает, что у оператора мало опыта работы с петлями на транковом боксе, но петлю удалось восстановить.

Довольный фрикер Эд заносит петлю в свой список работающих соединений. Эд великолепный исследователь. С невероятной дотошностью он распутывает лабиринты и хитросплетения телефонных соединений, выходит на подстанции и релейные узлы, чтобы найти одну-единственную бесплатную петлю. На это у него уходят многие дни и часы. Ему удалось составить список, состоящий из восьмисот номеров в сорока разных штатах, по которым можно звонить бесплатно из любой точки страны.

Исследователь Эд, девятнадцатилетний студент-инженер, также прекрасно разбирается в технике. В возрасте семнадцати лет он самостоятельно с нуля собрал работающий блю-бокс (в отличие от остальных, Эд не слепой). Этим вечером, раздав присутствующим последнюю версию своего списка бесплатных номеров (набранного шрифтом Брайля для слепых фрикеров), Эд сообщает о своем новом открытии:

— Наконец, все работает, я проверял. С помощью этой схемы любой телефон с тональным набором превращается в мультичастотник.

Тоновые сигналы, которые вы слышите в трубке, это совсем не те сигналы, которыми управляется междугородняя связь. Фрикеры считают, что AT&T специально разработала для телефонных аппаратов другой набор тонов, иначе каждый аппарат мог бы управлять междугородней коммутационной системой.

Схема Эда позволяет оснащать каждый телефон с тоновым набором шестью мастер-кодами, то есть по сути превращает его в блю-бокс.

Эд показывает мне схему и спецификацию радиодеталей:

— Собрать схему непросто, но все детали можно купить хоть в «Юном технике».

Эд интересуется у Ральфа, удалось ли тому восстановить конференц-связь с другими фрикерами. Последняя крупная конференция — историческая конференция «2111» — была проведена через неиспользуемый телексный транк где-то в дебрях коммутационного узла 4А в Ванкувере, Канада. В течение долгих месяцев фрикеры могли дозваниваться в Ванкувер, набирать «604» (код Ванкувера), а затем — «2111» (внутренний номер для телексного транка), чтобы в любое время дня и ночи очутиться в центре разговора других фрикеров из разных концов страны, операторов с Бермудских островов, Токио или Лондона, симпатизирующих фрикерам, разнообразных гостей и техников. На конференции обменивались огромным количеством разнообразной информации.

Фрикеры выпытывали друг у друга секреты и строили коварные планы против телефонных компаний. Ральф давал концерты «Мультичастотного буги» с помощью электрооргана, Капитан Кранч демонстрировал свою фрикерскую доблесть, делая «кругосветные» звонки, и пошлил по поводу своих подружек. (Капитан живет сразу несколькими фантазиями к восторгу слепых фрикеров, которые поощряют его на новые подвиги от имени их всех.) Немного нахальная фрикерская банда с Северо-запада учинила внутренние разборки прямо на конференции, развязав на некоторое время партизанскую войну; Карл, специалист по «международным тоновым отношениям» показал недавно обнаруженные прямые линии на остров Бахрейн в Персидском заливе, представил присутствующим своего нового друга — фрикера из Претории и объяснил принцип действия новых линий связи между Оклендом и Вьетнамом. (Многие фрикеры зарабатывают карманные деньги, помогая родственникам военнослужащих прозвониться во Вьетнам всего за пять долларов за час транстихоокеанского разговора.)

Сутки напролет линия в конференции была занята. Слепые фрикеры со всей страны, одинокие и изолированные в окружении зрячих братьев и сестер или запертые в компании других слепых в специальных школах, знали, что они в любое время могут позвонить на конференцию и перекинуться парой слов с такими же слепыми ребятами с другого конца Америки. По словам слепых, для них нет особой разницы разговаривать по телефону или сидя рядом друг с другом в одной комнате. Чисто физически в Ванкуверском узле связи находилась просто одна титановая пластина размером два на два. Но для слепых ребят быть «там» означало

восхитительное чувство общности с внешним миром, которого они добивались своим мастерством и умением.

Однако в прошлом году первого апреля Ванкуверская Конференция прекратила свое существование. Фрикеры предвидели это. Ванкуверские телефонные узлы переходили с пошаговой системы на систему 4А, и в процессе такого перехода телексную линию 2111 предполагалось закрыть. Фрикеры узнали точную дату отключения линии за неделю из внутренних переговоров служащих телефонной компании.

В течение последовавших безумных семи дней каждый американский фрикер сутками просиживал на номере 2111. Опытные фрикеры объясняли новичкам, как дозвониться до Конференции, чтобы те могли хоть понять, что это такое, пока Конференцию не отключили. Самые искушенные тщетно сканировали междугородние номера в поисках возможности установления новой конференц-линии. Наконец, ранним утром первого апреля все было кончено.

— У меня было предчувствие за пару часов до полуночи, — вспоминает Ральф. Было такое ощущение, что с линиями что-то творится. Какие-то помехи, писки, перерывы. Некоторые фрикеры были отключены и прозвонились снова. Некоторые обнаружили, что уже не могут дозвониться. Я потерял связь около часа ночи, но сумел снова дозвониться и удерживать линию до конца. Это произошло около четырех утра. Нас оставалось четверо на линии, когда конференции настал конец. Мы, конечно, снова пытались прозвониться, но без толку.

Легендарный Марк Бернэ оказывается «полуночным незнакомцем»

Марк Бернэ. Я встречал это имя и раньше. Я видел его в списке фрикеров Гилбертсона.

Калифорнийские фрикеры упоминали Марка Бернэ, как, возможно, первого и самого заслуженного фрикера Западного побережья. И действительно: практически каждый фрикер Запада США может проследить свою личную историю либо непосредственно к Марку Бернэ или кому-либо из его учеников.

Говорят, что пять лет тому назад этот самый Марк Бернэ (это псевдоним) разъезжал по всему Западному побережью, расклеивая в телефонных будках небольшие объявления.

В объявлениях было нечто вроде: «Хотите услышать интересную магнитофонную запись? Позвоните по указанным номерам». Указанные номера выводили на бесплатные петли. Когда любопытствующие звони-

ли по ним, они слышали предварительно записанный на магнитофон рассказ Бернэ о том, как пользоваться петлями. Бернэ также сообщал дополнительные номера петель и в завершение произносил следующее: «Сегодня вечером в шесть часов эта запись остановится, и вы с друзьями сможете испытать линию. Приятного времяпрепровождения».

— По началу я был разочарован низким числом звонящих, — сказал мне Бернэ, когда мне наконец удалось связаться с ним по одному из его многочисленных номеров. В начале разговора Бернэ, как и большинство других бывалых фрикеров, поспешил заверить меня, что «не делает ничего незаконного».

— Я не только облазил все побережье, расклеивая эти объявления, но даже по ночам разбрасывал их перед школами, оставлял в кондитерских лавках, расклеивал на главных улицах небольших городов. Поначалу никто особенно не интересовался. Я часами слушал линию, но никто не объявлялся. Я не мог понять, почему люди такие нелюбопытные. Наконец прозвонились две девчонки из Орегона, рассказали своим друзьям, и тут началось.

Еще до своих поездок Бернэ собрал вокруг себя на лос-анджелесских петлях внушительную группу фрикеров (эра блю-боксов еще не наступила). Бернэ не утверждает, что открыл эти самые петли. Пальму первооткрывателя он отдает восемнадцатилетнему школьнику из Лонг Бич, имя которого он забыл и который, как он утверждает, однажды «просто исчез». Когда Бернэ сам независимо от того парня обнаружил петли, основываясь на смутных намеках в старых номерах «Automatic Electric Technical Journal», выяснилось, что десятки друзей того парня-первооткрывателя уже давно пользовались петлями.

Тем не менее именно один из учеников Бернэ открыл для слепых мир фрикинга. Парень из Сиэтла, узнавший о петлях из магнитофонной записи Бернэ, рассказал своему слепому другу, а тот — другим слепым ребятам в зимнем лагере для слепых в Лос-Анджелесе.

Когда сезон в лагере закончился, и дети разъехались по домам, каждый привез в свой родной город недавно открытую тайну.

Именно так первые слепые познакомились с фрикингом. Для них, да и для большинства других фрикеров, открытие петель стало отправной точкой для изучения более сложных фрикерских методов, а также отличным средством для обмена опытом.

Год спустя один слепой парень, переехавший на Восток, привез с собой в летний лагерь для слепых в Вермонте секрет фрикинга.

Секрет распространился по всему Восточному побережью. И все изначально из объявления Марка Бернэ.

Бернэ, которому нынче около тридцати, увлекся фрикингом в возрасте пятнадцати лет, когда его семья переехала жить в пригород Лос-Анджелеса, телефонная сеть которого была построена на оборудовании «General Telephone and Electronics». Он был очарован различиями между оборудованием «Bell» и «G.T.&E». Он обнаружил, что особым образом нажимая на рычаг телефона, можно вытворять занятные фокусы. Он научился отличать мельчайшие различия в щелчках и шорохах, слышимых в линии. Он узнал, что может обойти реле телефонной зоны Лос-Анджелеса, если будет правильно совмещать нажатия на рычаг телефона с определенными щелчками в линии. Независимые телефонные компании — их существует еще около 1900, большая часть является лишь осколками огромной империи Ма Белл — всегда были излюбленным объектом для фрикинга, сначала в качестве инструмента познания, а позже — как трамплин для манипуляций с громадной системой Белл. Фрикер, находящийся на территории Ма Белл, может прозвониться в систему какой-нибудь независимой компании и через нее получить контроль над системой Белл.

— Я просто влюблен в электронику, — говорит Бернэ. Там столько возможностей для манипуляций. Столько интересных поломок.

Вскоре после этого Бернэ закончил колледж (получив сразу две специальности: по химии и философии). В это же время Бернэ переключился с системы «G.T.&E.» на Белл, совершил свое легендарное путешествие с расклеиванием объявлений и в конце концов обосновался на Северо-западе тихоокеанского побережья. Он обнаружил, что хотя Белл и не ломается так часто, как «G.T.&E.», там тоже есть достаточно возможностей «поэкспериментировать».

Бернэ освоил блю-боксы. Он создал свою собственную лабораторию по изучению телефонных систем. Он продолжал свою проповедническую деятельность, расклеивая объявления. Он установил два телефонных номера, один с записью наставлений начинающим фрикерам, второй — с последними новостями и техническими новинками, собранными со всей страны.

Сейчас, как признался мне сам Бернэ, он больше не занимается фрикингом в чистом виде. «В последнее время мне больше нравится играть с компьютером, чем с телефоном».

— Мое кредо по отношению к компьютерам такое же, как и к телефонам — узнать, как одержать верх над системой, как узнать то, что я, по идее, не должен знать, как заставить систему делать то, что она, по идее, не должна делать.

На самом деле, как признался Бернэ, его недавно уволили с работы (он работал программистом) за то, что он слишком вольно обращался с системой. Он обслуживал центральный сервер крупной корпорации, доступ к которому имели так же другие компании.

Доступ разрешался только тем программистам и компаниям, которые имели специальные пароли. При этом каждый пароль позволял пользователю работать только с отдельной частью сервера. Такая система паролей предотвращала хищение информации компаниями друг у друга.

— Я смог написать программу, позволяющую расшифровывать пароли всех пользователей, — сообщает Бернэ. Я начал развлекаться с этими паролями. Намекал пользователям системы, что я знаю их пароли. Я подбрасывал администраторам системы записки, рассказывающие о моем знании, с подписью «Полуночный Незнакомец».

Я все больше и больше изощрялся, давая им понять о своих потенциальных возможностях. Я более чем уверен, что они и представить не могли, на что я способен. Но ответа я не получал.

Они регулярно меняли пароли, но я узнавал новые пароли и давал им это понять. Но они так ни разу и не ответили непосредственно Полуночному Незнакомцу.

В конце концов я написал программу, которая предотвращала возможность вычисления паролей. В сущности я подсказал им, как уничтожить меня, Полуночного Незнакомца. Это была очень изящная программа. Я стал оставлять улики. Я хотел, чтобы они воспользовались программой, а я в свою очередь создал бы что-нибудь еще более продвинутое, чтобы обойти ее. Но они не хотели играть в эти игры.

Я хотел, чтобы меня поймали. То есть я, конечно, не хотел, чтобы меня лично поймали, но я хотел, чтобы они заметили меня и признали мое существование. Я хотел, чтобы они хоть как-нибудь ответили.

В конце концов инженеры системы достаточно озаботились безопасностью информации в системе. Но вместо того, чтобы ответить Полуночному Незнакомцу в его элегантной манере, они призвали на помощь службу безопасности, допросили всех сотрудников, нашли стукача, который раскрыл личность Полуночного Незнакомца и уволили его.

— Поначалу служба безопасности советовала компании нанять меня на полный рабочий день, чтобы найти другие дыры в системе и других компьютерных фрикеров. Я может быть на это и согласился бы. Но я скорее всего стал бы тройным агентом, а не двойным, как они того хотели. Наверное, я попытался бы воскресить Полуночного Незнакомца и

ловил бы сам себя. Кто знает. В любом случае начальство не приняло эту идею.

Говорят, что, сидя дома, можно залезть в банк данных ФБР

Компьютерный фрикинг может стать новым масштабным явлением. Он полностью соответствует чаяниям телефонных фрикеров. Гилбертсон, изобретатель блю-бокса и извечный фрикер, тоже переключился с телефонного фрикинга на компьютерный. До вовлечения в бизнес по производству блю-боксов Гилбертсон, высококвалифицированный программист, разрабатывал программы для операций на международном фондовом рынке.

Но всерьез заниматься компьютерами он начал, когда узнал, что может использовать блю-бокс в тандеме с терминалом, установленным на его рабочем месте. Терминал и клавиатура были оснащены устройством акустического совмещения, и соединив телефонный аппарат с терминалом, а затем блю-бокс с телефонным аппаратом, Гилбертсон мог устанавливать удаленное соединение с другими компьютерами при сохранении полной анонимности и бесплатно, программировать такие компьютеры без каких-либо ограничений, загружать в них ложную информацию, скачивать различные данные. Он объяснил мне, что подключается к компьютерам следующим образом: занимает все линии, подключается к тестовому транку и подслушивает пароли пользователей системы, а потом имитирует их сигналами блю-бокса.

Гилбертсон говорит, что нет ничего невозможного в том, чтобы залезть в центральный банк данных ФБР через терминал местного отделения полиции и «подправить» некоторые данные в архивах ФБР.

Он утверждает, что таким образом однажды смог перепрограммировать центральный компьютер одного учреждения, и благодаря этому целая часть сети была отведена для его личного использования, при этом будучи скрытой от посторонних глаз. Мне однако не удалось перепроверить подлинность этой информации.

Как и Капитан Кранч, как Александр Грэм Белл (псевдоним одного инженера с Восточного побережья, который утверждает, что изобрел блэк-бокс, и продает блэк- и блю-боксы игрокам в азартные игры и радикалам-подпольщикам), как большинство телефонных фрикеров, Гилбертсон начал свою «карьеру» в подростковом возрасте, пытаясь взломать телефоны-автоматы. Сперва изучить, а потом взломать. Обрядом посвящения во фрикеры было достать десятицентовую монету из телефона-автомата. Освоив восемнадцать основных способов по извлечению

монет из автоматов, Гилбертсон также научился делать мастер-ключи к контейнерам с монетами и мог теперь доставать не только свои монеты.

Он где-то украл телефонное оборудование и собрал дома свой собственный коммутационный узел. Он научился делать простой «брэдбокс», какой использовался букмекерами в тридцатые годы (букмекер давал номер своим клиентам-игрокам; телефон с этим номеров устанавливался в квартире у какой-нибудь старой вдовы, но подключался к аппарату в конторе букмекера на другом конце города; и когда полицейские выслеживали номер, они находили всего лишь старую вдову.

Через некоторое время после того дня, когда в глубинах технической библиотеки Гилбертсон наткнулся на журнал с описанием частот управляющих сигналов телефонной системы и собрал свой первый блюбокс, через некоторое время после этого Гилбертсон прервал многообещающую карьеру в области химии и начал торговать блю-боксами по $1 500 за штуку.

— Мне пришлось оставить химию. Мне стало там просто скучно, — сказал он мне однажды вечером. Мы беседовали в гостях у человека, служившего посредником между Гилбертсоном и синдикатом в сделке по продаже блю-боксов на сумму $300 000, которая провалилась из-за юридических неувязок. В комнате курили.

— Ничего интересного узнать я там больше не мог, — продолжал он. Химия становится скучным предметом, когда добираешься до самых вершин. Я не знаю. Я, наверное, не смогу объяснить, почему там скучно. Это нужно самому испытать. Но в то же самое время ты получаешь, я не знаю, ложное чувство всемогущества. В этом смысле химия похожа на фрикинг. Вся система под контролем. И в системе есть дыры, и ты проникаешь через эти дыры, как Алиса из сказки Кэрролла, и ты притворяешься, что на самом деле ничего предосудительного не делаешь, или по крайней мере это не совсем ты, кто вытворяет все фокусы. Чистой воды Льюис Кэрролл. Химия и фрикинг. Наверное поэтому среди фрикеров попадаются псевдонимы типа «Чеширский Кот», «Червовый Король» или «Снарк». Но во фрикинге есть нечто, чего не найдешь в химии. Он поднимает на меня взгляд:

— Ты когда-нибудь что-нибудь крал?

— Ну-у-у... да, я...

— Тогда ты можешь все понять! Ты знаешь то чувство, которое овладевает тобой. Это не просто знание, как в химии. Это запретное знание. Можно узнать все обо всем под солнцем и умереть со скуки. Но зная, что это незаконно... Смотри: можно быть маленьким, но умным и

шустрым и при этом надувать кого-нибудь большого, сильного и очень опасного.

Люди типа Гилбертсона и Александра Грэма Белла постоянно говорят об обмане телефонных компаний и взломе Ма Белл. Но если им показать одну-единственную кнопку, нажав на которую можно превратить всю систему связи AT&T в кучу обломков, они вряд ли нажмут на эту кнопку. Фрикеру нужна телефонная сеть так же, как католику нужна церковь, как Сатане нужен Господь, как Полуночному Незнакомцу больше всего нужно было внимание со стороны операторов компьютера.

Позже тем вечером Гилбертсон закончил свой рассказ о том восторге, который он испытал, когда блю-боксы заполонили страну, когда он понял, что «на этот раз телефонисты сели в лужу». Неожиданно он сменил тему.

Разумеется, я одновременно люблю и ненавижу Ма Белл. Мне она даже чем-то нравится. Наверное, я бы очень расстроился, если бы компания распалась на несколько более мелких организаций. Есть что-то привлекательное в том, что при всем ее великолепии, в системе находится множество недостатков. Именно благодаря таким недостаткам я могу проникнуть в систему. В этом есть что-то завораживающее, заставляющее тебя искать новых встреч с системой. Я спрашиваю, что произойдет, когда все запретные тайны телефонной системы будут познаны.

— Не могу точно сказать, может быть устроюсь туда на работу на некоторое время.

— Может быть даже в службу безопасности?

— Да, я именно так бы и поступил. Мне безразлично, на какой стороне выступать.

— Что, и ты даже помогал бы вычислять других фрикеров? — спросил я, вспомнив развлечение Марка Бернэ.

— Да, это было бы занятно. Да, я смог бы обхитрить многих фрикеров. Конечно, если бы я достиг высокого уровня мастерства в этом деле, мне снова стало бы скучно. И тогда пришлось бы надеяться, что появятся еще более изощренные фрикеры, чем я. Это внесло бы определенный интерес в игру. Может, мне даже пришлось бы их выручать. Ну, ребята, мне не хотелось бы, чтобы это стало известно всем, но не пробовали ли вы?... Игру можно было бы все усложнять и усложнять.

Дилер первый раз за вечер вступает в разговор. Все это время он смотрел на переливающиеся узоры на стене, выложенной цветной плиткой с иллюминацией. (На самом деле никаких узоров там нет: цвет и яр-

кость каждой плитки определяются компьютерным генератором произвольных чисел, собранным Гилбертсоном и следящим за тем, чтобы рисунок на плитках не повторялся.)

— То, о чем вы говорите, это милые игры, — говорит дилер товарищу. — Но я не был бы против, если бы фрикерам хорошенько врезали. Телефон потерял всякую конфиденциальность. Нельзя свободно говорить по телефону, о чем хочешь, надо прибегать ко всем этим параноидальным штучкам. Круто ли говорить по телефону? То есть, даже если это и круто, если вам приходится спрашивать «круто ли это», то это уже не круто. Как те слепые пацаны, люди будут строить свои собственные телефонные сети, если они хотят вести конфиденциальные разговоры. Остальное вы знаете. В линии вы больше не услышите тишины. У них на межгороде установлена система разделения: вы прерываете на время разговор, а они на время паузы занимают вашу линию под чей-нибудь еще разговор. Вместо паузы, когда кто-нибудь дышит в трубку или вздыхает, вы слышите пустоту, и связь восстанавливается только после первого произнесенного слова, начало которого тоже может быть обрезано. Тишина в расчет не берется: вы оплачиваете длительность всего разговора, а они у вас отнимают паузы. Говорить не круто, и поэтому вы не слышите человека, когда он молчит. Что в этом телефоне хорошего? Пусть им всем врежут.

Аресты в Мемфисе

Джо Энгрессиа никогда не хотел мешать Ма Белл. Он всегда мечтал там работать.

В тот день, когда я навестил Джо в его тесной квартирке в Мемфисе, он был огорчен очередным отказом в приеме на работу в телефонной компании.

— Они специально затягивают. Сегодня я получил письмо о том, что они вынуждены отсрочить интервью. Мне письмо хозяин дома прочитал. Они привели какую-то отговорку насчет получения бумаг о моей инвалидности, но мне кажется, что причина совсем не в этом.

Я включил 40 Вт лампочку в комнате Джо — он иногда забывает сделать это при посещениях гостей — в комнате было столько оборудования, что можно было открывать маленькую телефонную станцию.

Один телефон стоит у него на столе, второй — в открытом выдвижном ящике стола. Рядом с настольным телефоном лежит мультичастотник с крупными кнопками размером с сигаретную пачку, а рядом с ним — какое-то устройство с клеммами и зажимами «крокодилами». Тут же размещается печатная машинка со шрифтом Брайля. На полу возле

стола вверх дном, как дохлая черепаха, лежит наполовину выпотрошенный корпус старого эбонитового телефона. В другом углу комнаты на драном пыльном диване лежат еще два телефона, один из которых с тональным набором номера; два магнитофона; куча телефонных деталей и кассет и игрушечный телефон в натуральную величину.

Наш разговор прерывается каждые десять минут звонками фрикеров со всей страны, в комнате Джо трезвонит все за исключением разве что игрушечного телефона и печатной машинки Брайля. Один четырнадцатилетний слепой пацан из Коннектикута звонит и сообщает, что у него появилась подружка. Он хочет поболтать с Джо о подружках. Джо говорит ему, что они созвонятся позже вечером, когда будут одни на линии.

Джо делает глубокий вдох и свистит в трубку с частотой 2600. Джо приятно, когда ему звонят, но этим вечером он чем-то обеспокоен и нахмурен. Помимо отказа от приема на работу он еще узнал сегодня, что дом, где он снимает квартиру, подлежит сносу в течение двух месяцев в связи с реконструкцией квартала. Невзирая на всю свою убогость, квартира на Юнион Авеню была первым собственным пристанищем Джо, и он боится, что не успеет найти себе новую квартиру до сноса этой.

Но что действительно заботит Джо, так это то, что телефонисты не слушают его.

— Недавно я проверял бесплатные (800) номера и обнаружил, что по некоторым номерам в Нью Хэмпшире нельзя прозвониться из Миссури и Канзаса. Мелочь, конечно, но меня такие неполадки раздражают, я начинаю плохо думать о всей системе связи. Ну, так я позвонил на АТС и сообщил о неполадке, а они — ноль внимания.

Сегодня я разговаривал с ними в третий раз, и вместо того, чтобы все исправить, они на меня наорали. Меня это бесит: я пытаюсь им помочь, а они... Никак не могу понять их логику: ты пытаешься им помочь, а они говорят, что ты мошенник, обманывающий телефонную компанию.

Одним воскресным вечером Джо пригласил меня отужинать в отеле Холидэй Инн. Джо часто по воскресеньям выгребает из копилки деньги, заказывает такси и едет ужинать в один из тринадцати ресторанов Холидэй Инн в Мемфисе. (В Мемфисе находится штаб-квартира Холидэй Инн. Джо любит эти гостиницы с тех пор, как впервые в одиночку съездил в Джексонвилл, Флорида, с целью изучения станционного оборудования Белл и останавливался в номере Холидэй Инн.)

Он любит эти отели за то, что они символизируют для него свободу, а также потому, что в этих гостиницах по всей стране обстановка в номерах одна и та же, и Джо чувствует себя там, как дома. Почти, как на телефонной станции.

За ужином в ресторане Pinnacle медицинского центра Холидэй Инн на Мэдисон Авеню в Мемфисе Джо рассказывает мне о ключевых моментах своей жизни как фрикера.

В возрасте семи лет Джо научился первому фокусу с телефоном.

Злобная нянька, устав от возни Джо с телефонным аппаратом, поставила замок на диск телефона. «Меня это так взбесило. Стоит телефон, а я не могу им воспользоваться... И в ярости я стал поднимать и бросать трубку. И тут я заметил, что если бросить трубку один раз, телефон наберет цифру «1». Ну я попробовал стукнуть по рычагу два раза...» Через несколько минут Джо уже умел набирать номер при помощи повторных нажатий на рычаг аппарата. «Меня обуял такой восторг. Я даже сейчас помню, как я смеялся и уронил телефон на пол».

В восемь Джо научился свистеть. «Однажды я слушал, как автоматический голос сообщал, что такой-то номер в Лос-Анджелесе не работает — я уже тогда в столь нежном возрасте звонил в Лос-Анджелес, но главным образом по неработающим номерам, так как такие звонки были бесплатными, и днями слушал робота-автоответчика. Ну, я одновременно и свистел, потому что слушать магнитофонную запись достаточно скучно, даже если она из Лос-Анджелеса, и неожиданно в процессе моего свиста запись отключилась. Я попробовал посвистеть еще, и произошло то же самое. Тогда я позвонил на АТС и сказал буквально следующее:

— Меня зовут Джо. Мне восемь лет и я хочу знать, почему, когда я насвистываю мелодию, телефон отключается. Мне попытались объяснить, но я мало что понял — слишком много технических подробностей. Я продолжал свои исследования, и никто не мог помешать мне заниматься любимым делом. Телефон был моей жизнью, я знал, что могу попасть в тюрьму, но я готов был заплатить любую цену за то, чтобы продолжать заниматься любимым делом.

Когда мы только входили в квартиру Джо на Юнион Авеню, раздался телефонный звонок. Звонил Капитан Кранч. Капитан следил за мной по пятам, звоня во все места, посещаемые мной, и рассказывая мне о фрикерах, с которыми я знакомился. По словам Капитана, на этот раз он звонил из места, которое он сам описал как «нычка в горах Сьерра Невада». Он выпаливает залпы мультичастотных тонов и сообщает Джо, что сегодня вечером собирается заняться делом.

— Пофрикать по особенному, — как он выразился. Джо хихикнул.

Капитан напомнил мне, что то, что он говорил о возможности парализовать телефонную сеть всей страны, было сущей правдой, хотя ни он, ни другие фрикеры не применяли это умение для саботажа.

Они лишь узнали о такой возможности, чтобы помочь телефонным компаниям.

— Мы им сильно помогаем. Например, в случае с неполадкой на линии Нью Хэмпшир/Миссури. Мы помогаем им даже больше, чем они знают.

После того, как мы прощаемся с Капитаном и Джо «отсвистывает» его от линии, Джо рассказывает мне о своем сне, который беспокоил его предыдущей ночью: «Меня поймали и посадили в тюрьму. Меня долго везли. Везли в тюрьму далеко-далеко отсюда».

Мы остановились на ночь в Холидэй Инн, и это была моя последняя возможность потрогать телефон, и я все плакал, и горничная гостиницы сказала мне: «Послушай, дорогой, в Холидэй Инн нельзя плакать. Здесь надо всегда улыбаться. Особенно в свою последнюю ночь здесь». Мне от этих слов стало только горше и я плакал до изнеможения.

Через две недели после того, как я попрощался с Джо Энгрессиа, сотрудники службы безопасности телефонной компании и Мемфисской полиции ворвались в квартиру Джо.

Потрясая ордером, который они позже прикололи к стене, они конфисковали все оборудование в квартире, включая игрушечный телефон. Джо поместили под арест и отвезли в городскую тюрьму, где он провел ночь, так как не имел ни денег, ни друзей в Мемфисе, которые могли бы внести за него залог.

Не совсем ясно, с кем и о чем говорил Джо в ту ночь, но кто-то однозначно сказал ему, что телефонная компания имела неоспоримые улики против него, благодаря признаниям, которые Джо сделал тайному агенту компании.

К утру Джо был убежден, что журналист из Эсквайра, с которым он беседовал пару недель тому назад, и был тем тайным агентом.

Можно только представить, что он думал о человеке, которого он не мог видеть и который коварно втерся в его доверие, слушал признания Джо о его мечтах и снах с единственной целью упечь его за решетку.

— Я действительно думал, что это был журналист, — сказал Энгрессиа на пресс-конференции в Мемфисе. — Я ему все выложил... —

Чувствуя себя преданным, Джо продолжал свои признания полиции и прессе.

Как выяснилось, телефонная компания на самом деле использовала тайного агента для уличения Джо, хотя это и не был журналист из Эсквайра.

Занятно, что агенты безопасности всполошились и начали собирать дело на Джо из-за одного из его проявлений любви к системе: Джо позвонил в техническую службу компании и сообщил, что обнаружил группу поврежденных междугородних транков, а также пожаловался на повреждение линии Нью Хэмпшир/Миссури. Джо всегда любил линии Ма Белл за их чистоту и надежную работу.

Подозрительный телефонист сообщил о Джо службе безопасности, которые выяснили, что на имя Джо никогда не выставлялись счета за межгород.

Потом агенты узнали, что Джо собирается совершить экскурсию на местную АТС, и поместили туда одного из своих людей. Он прикинулся телефонистом-стажером и водил Джо по станции. Он был крайне приветлив и учтив. По окончании экскурсии агент предложил Джо подвезти его до дома и по дороге спросил — «как технарь технаря» — о «тех самых блю-боксах», о которых столько говорят.

Джо говорил о блю-боксах без опаски и хвастался другими своими достижениями.

На следующее утро служба безопасности телефонной компании установила на линию Джо записывающее устройство, которое в конце концов зафиксировало незаконный звонок. Тогда они запросили ордер на обыск и ворвались в квартиру.

На суде Джо отрицал свою вину в обладании блю-боксом и краже услуг у телефонной компании. Сочувствующий судья сузил спектр обвинений до злостного хулиганства и признал Джо виновным по этому пункту, приговорив к двум месячным срокам условно, обязав Джо более никогда не хулиганить с телефоном. Джо пообещал, но телефонная компания отказалась включать Джо телефон. В течение двух недель после суда до Джо нельзя было дозвониться иначе как по телефону-автомату в подъезде, причем хозяин дома вел учет всех звонков.

Фрикер по имени Карл смог связаться с Джо после суда и сказал, что тот был практически повержен всей этой историей.

— Больше всего меня беспокоит, — сказал мне Карл, — что на этот раз Джо говорил правду.

Я имею в виду его обещание. Что он больше никогда не будет заниматься фрикингом. Он мне то же самое сказал. Что больше никогда. Никогда в жизни. Он сказал, что они настолько пристально за ним следят, что он и шелохнуться не может, чтобы не угодить прямо за решетку. При мыслях о тюрьме он просто впадает в депрессию. Его невозможно было слушать, когда он говорил об этом. Я не знаю. Может ему от этого становилось легче. Хотя бы по телефону. Карл сообщил также, что все фрикерское сообщество ополчилось на ту телефонную компанию за ее отношение к Джо. «Все то время, пока Джо жил мечтой о получении работы на телефонной компании, они собирали на него досье. Меня это просто бесит. Джо большую часть жизни потратил, помогая им. Ублюдки. Они полагают, что история с Джо может послужить уроком остальным. Ни с того ни с сего они стали донимать нас тут на побережье. Агенты прослушивают линии. Они только что наехали на одного парня и отрезали ему связь. Но как бы Джо не повел себя дальше, мы больше не будем терпеть эту ложь». Примерно две недели спустя у меня звонит телефон и около десятка фрикеров по очереди приветствуют меня из разных точек страны. Среди них Карл, Эд и Капитан Кранч. С помощью недовольного жизнью телефониста восстановлена всеамериканская фрикерская конференция через АТС города ***.

— Сегодня у нас в гостях особый человек, — говорит Карл.

Я слышу голос Джо. Он счастливым голосом сообщает, что переехал в местечко под названием Миллингтон, Теннеси, за пятнадцать миль от Мемфиса, и получил работу в качестве мастера по ремонту телефонных аппаратов в небольшой независимой компании.

Он надеется, что однажды получит место оператора-телефониста.

— Именно о такой работе я мечтал. Они узнали обо мне из всей той шумихи вокруг процесса. Может быть Ма Белл невольно оказала мне добрую услугу, арестовав меня. Только подумать: целый день у меня в руках будут телефоны.

— Ты слышал выражение: «Не плюй в колодец?» — спрашивает меня фрикер Карл. Так вот я думаю, они скоро сильно пожалеют о своем поступке по отношению к Джо и остальным нам.

Чтение пейджерных сообщений с помощью компьютера

Чтение пейджерных сообщений практически любой российской пейджерной компании с применением компьютера не составляет ника-

кого труда. Также легко осуществляется и передача на любой пейджер. Но вы должны знать — ЛЮБОЕ использование полученной таким образом информации против третьих лиц является преступлением. Вы должны использовать информацию, представленную ниже, ТОЛЬКО для радиолюбительских целей! За рубежом радиолюбительский пейджинг является очень популярным увлечением.

Многие радиолюбители на своих сайтах предлагают рекристаллинг (замену кварцевого резонатора) для перестройки пейджера на любительский диапазон. Стоит это у них порядка 20 долларов с пересылкой по почте. О сколько-нибудь серьезном развитии любительского пейджинга в России пока ничего не известно. Вам потребуется:

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

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

3. Собственно программа. Рекомендую POC32. В документации к программе подробно описаны подключение и настройка, поэтому не буду повторяться. Коротко изложу несколько важных моментов. Программа прекрасно работает на прием со всеми звуковыми картами, обеспечивающими качественную запись звука.

Но для устойчивого декодирования ОБЯЗАТЕЛЬНО надо подключать линейный вход саундкарты непосредственно к выходу дискриминатора приемника. При прохождении через УНЧ фронты сигнала значительно искажаются и читаемость сообщений всего 7–8%, а с дискриминатора — 99–100% при тех же условиях приема. Будьте очень аккуратны при работе.

Программа потребует настройки кодовой таблицы (их может быть несколько). Начальная таблица имеет имя Default.tbl. Сделайте ее копию и начинайте настраивать. Запустите программу на прием сообщений. Во встроенном блокноте Windows Notepad откройте ваш файл кодовой таблицы. Столбец слева — принимаемый код, справа — его отображение на экране.

Посмотрите на принимаемых сообщениях, какие буквы нужно исправлять, и замените их в кодовой таблице. Сохраните файл и переустановите его в меню Properties. При необходимости повторите процесс.

Проблема в том, что даже в одной пейджинговой компании могут быть пейджеры разных типов, с разными кодировками. Например, с

транслитерацией, когда русские слова пишут латинскими буквами. Они различаются диапазоном номеров либо номером функции.

Одновременно правильно декодировать сообщения для разных систем не получится, так как действует только одна таблица кодов, не переключаемая динамически. Этот недостаток программы, вероятно, будет вскоре исправлен.

Безопасность связи

Так уж устроен мир, что любое техническое изобретение человеческого разума, расширяющее наши возможности и создающее для нас дополнительный комфорт, неизбежно содержит в себе и отрицательные стороны, которые могут представлять потенциальную опасность для пользователя. Не являются исключением в этом плане и современные средства беспроводной персональной связи. Да, они несоизмеримо расширили нашу свободу, отвязав нас от телефонного аппарата на рабочем столе и дав нам возможность в любое время и в любом месте связаться с необходимым корреспондентом. Но немногие знают, что эти «чудеса техники» скрывают в себе весьма опасные «ловушки». И для того, чтобы однажды ваш помощник (скажем, сотовый телефон) не превратился в вашего врага, эти «ловушки» следует хорошо изучить.

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

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

Сотовые телефоны

Мобильные телефоны сотовой связи фактически являются сложной миниатюрной приемо-передающей радиостанцией. Каждому сотовому телефонному аппарату присваивается свой электронный серийный номер (ESN), который кодируется в микрочипе телефона при его изготовлении и сообщается изготовителями аппаратуры специалистам, осуществляющим его обслуживание. Кроме того, некоторые изготовители указывают этот номер в руководстве для пользователя. При подключении аппарата к сотовой системе связи, техники компании, предоставляющей услуги этой связи, дополнительно заносят в микрочип телефона еще и мобильный идентификационный номер (MIN). Мобильный сотовый телефон имеет большую, а иногда и неограниченную дальность действия, которую обеспечивает сотовая структура зон связи. Вся терри-

тория, обслуживаемая сотовой системой связи, разделена на отдельные, прилегающие друг к другу, зоны связи или «соты».

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

Периодически (с интервалом 30–60 минут) базовая станция излучает служебный сигнал. Приняв его, мобильный телефон автоматически добавляет к нему свои MIN- и ESN-номера и передает получившуюся кодовую комбинацию на базовую станцию. В результате этого осуществляется идентификация конкретного сотового телефона, номера счета его владельца и привязка аппарата к определенной зоне, в которой он находится в данный момент времени. Когда пользователь звонит по своему телефону, базовая станция выделяет ему одну из свободных частот той зоны, в которой он находится, вносит соответствующие изменения в его счет и передает его вызов по назначению. В случае, если мобильный пользователь во время разговора перемещается из одной зоны связи в другую, базовая станция покидаемой зоны автоматически переводит сигнал на свободную частоту новой зоны.

Пейджеры

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

Беспроводные радиотелефоны

Стационарный беспроводный радиотелефон объединяет в себе обычный проводный телефон, представленный самим аппаратом, подключенным к телефонной сети, и приемопередающее радиоустройство в виде телефонной трубки, обеспечивающей двусторонний обмен сигналами с базовым аппаратом. В зависимости от типа радиотелефона, дальность связи между трубкой и аппаратом, с учетом наличия помех и переотражающих поверхностей, составляет в среднем до 50 метров.

Проблема безопасности при пользовании сотовым телефоном и другими мобильными средствами персональной беспроводной связи

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

Проблемы защиты

Вы, наверное, не раз слышали рекламу компаний, предоставляющих услуги сотовой связи: «Надежная связь по доступной цене!». Давайте проанализируем, действительно ли она так уж надежна. С технической точки зрения — да. А с точки зрения безопасности передаваемой информации?

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

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

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

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

Принцип передачи информации такими устройствами основан на излучении в эфир радиосигнала, поэтому любой человек, настроив соответствующее радиоприемное устройство на ту же частоту, может услышать каждое ваше слово. Для этого даже не нужно иметь особо сложной аппаратуры. Разговор, ведущийся с сотового телефона, может быть прослушан с помощью продающихся на Западе программируемых сканеров с полосой приема 30 КГц, способных осуществлять поиск в диапазоне 860–890 МГц. Для этой же цели можно использовать и обычные сканеры после их небольшой модификации, которая, кстати, весьма подробно описана в Интернет. Перехватить разговор можно даже путем медленной

перестройки УКВ-тюнера в телевизорах старых моделей в верхней полосе телевизионных каналов (от 67 до 69), а иногда и с помощью обычного радиотюнера. Наконец, такой перехват можно осуществить с помощью ПК.

Легче всего перехватываются неподвижные или стационарные сотовые телефоны, труднее — мобильные, так как перемещение абонента в процессе разговора 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 карт или персональные идентификационные номера PIN), то они могут быть легко перехвачены с помощью того же цифрового сканера.

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

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

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

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 и GOLAY. Существует также целый ряд программных средств, которые позволяют ПК в сочетании со сканером автоматически захватывать рабочую частоту нужного пейджера или контролировать весь обмен в конкретном канале пейджинговой связи. Эти программы предусматривают возможность перехвата до 5000 пейджеров одновременно и хранение всей переданной на них информации.

Фрикинг

Фрикинг (мошенничество) в сотовых системах связи, известное еще под названием «клонирование», основано на том, что абонент использует чужой идентификационный номер (а, следовательно, и счет) в корыстных интересах. В связи с развитием быстродействующих цифровых сотовых технологий, способы мошенничества становятся все более изощренными, но общая схема их такова: мошенники перехватывают с помощью сканеров идентифицирующий сигнал чужого телефона, которым он отвечает на запрос базовой станции, выделяют из него идентификационные номера MIN и ESN и перепрограммируют этими номерами микрочип своего телефона. В результате, стоимость разговора с этого аппарата заносится базовой станцией на счет того абонента, у которого эти номера были украдены.

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

Кража номеров осуществляется, как правило, в деловых районах и в местах скопления большого количества людей: дорожные пробки на шоссе, 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.

Местоположение абонента

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

Текущее положение может выявляться двумя способами. Первым из них является обычный метод триангуляции (пеленгования), определяющий направление на работающий передатчик из нескольких (обычно трех) точек и дающий засечку местоположения источника радиосигналов. Необходимая для этого аппаратура хорошо разработана, обладает высокой точностью и вполне доступна.

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

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

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

Советы

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

Для предотвращения перехвата информации:

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

Помните, что труднее перехватить разговор, который ведется с движущегося автомобиля, так как расстояние между ним и перехватывающей аппаратурой (если та находится не в автомобиле) увеличивается и сигнал ослабевает. Кроме того, при этом ваш сигнал переводится с одной базовой станции на другую с одновременной сменой рабочей частоты, что не позволяет перехватить весь разговор целиком, поскольку для нахождения этой новой частоты требуется время.

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

Используйте, при возможности, цифровые сотовые телефоны.

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

В случае использования беспроводного радиотелефона:

- при покупке выясните, какую защиту он предусматривает;

- используйте радиотелефоны с автоматической сменой рабочих частот типа «spread spectrum» или цифровые, работающие на частотах порядка 900 МГц;
- по возможности, используйте радиотелефоны со встроенным чипом для шифрования сигнала.

Для предотвращения мошенничества:

- узнайте у фирмы-производителя, какие средства против мошенничества интегрированы в ваш аппарат;
- держите документы с ESN-номером вашего телефона в надежном месте;
- ежемесячно и тщательно проверяйте счета на пользование сотовой связью;
- в случае кражи или пропажи вашего сотового телефона сразу предупредите фирму, предоставляющую вам услуги сотовой связи;
- держите телефон отключенным до того момента, пока вы не решили им воспользоваться. Этот способ самый легкий и дешевый, но следует помнить, что для опытного специалиста достаточно одного вашего выхода на связь, чтобы выявить MIN/ESN номера вашего аппарата;
- регулярно меняйте через компанию, предоставляющую вам услуги сотовой связи, MIN-номер вашего аппарата. Этот способ несколько сложнее предыдущего и требует времени;
- попросите компанию, предоставляющую вам услуги сотовой связи, установить для вашего телефона дополнительный 4-х значный PIN-код, набираемый перед разговором. Этот код затрудняет деятельность мошенников, так как они обычно перехватывают только MIN и ESN номера, но, к сожалению, небольшая модификация аппаратуры перехвата позволяет выявить и его;
- наиболее эффективным методом противодействия является шифрование MIN/ESN номера (вместе с голосовым сигналом) по случайному закону.

Эмулятор SIM-карточки сотовых телефонов

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

1. Самый крутой путь — достать где-то чистые SIM-карточки, которые предназначены для сотовых операторов. Правда, они не совсем чистые, на них должен быть уже зашит криптографический алгоритм COMP128, и надо иметь для этих карточек вразумительную инструкцию по программированию шифровального ключа Ki. Дело в том, что в разных SIM-карточках ключ может находиться в совершенно разных местах. Что касается криптографического алгоритма, то он тоже может прошиваться в разных местах на карточке (нет единого стандарта, да он и ни к чему). Крипто-алгоритм (в данном случае COMP128) обычно находится в масочном ПЗУ карточки, и любой доступ к нему извне закрыт. Было бы, конечно, хорошо, если бы его можно было оттуда выдрать, но это невозможно!

Программа алгоритма написана на спец-ассемблере с применением других специальных средств и поэтому имеет чрезвычайно маленький объем (чуть более 1 Кб), для работы ей достаточно всего 128 байт ОЗУ. Скорость вычисления результата 0,6 секунды (650 000 операций).

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

2. В случае, если найдутся крутые программисты, которые смогут на ассемблере и с учетом специфических особенностей операционной системы процессорных смарткарт стандарта ISO 7816 реализовать опубликованный теперь и ставший широким достоянием хакеров всего мира алгоритм COMP128 так, чтобы после компиляции программа занимала не более 2 Кб и могла спокойно работать с оперативной памятью 128 байт, то останется только заняться поисками подходящего типа процессорной смарткарты (а в них обычно используется процессор 8051 или 6805 производства фирмы Motorola или SGS Thomson). При желании, можно доставать такие карты (чистые, без крипто-алгоритма DES или какого-либо другого) по средней цене 10–15 долларов за штуку. Эти карточки будут иметь процессор 6805 или 8051, ОЗУ 128 байт, ПЗУ 6 Кб, ППЗУ 3 Кб. В крайнем случае, можно достать более дорогие карты на базе процессора Motorola MC68HC05SC48 с ОЗУ 240 байт, ПЗУ 13 Кб и ППЗУ 8 Кб. Далее будем думать, как зашить в них эту программу крипто-алгоритма, шифровальный ключ Ki, а также мобильный номер IMSI.

3. Самый реальный путь — сделать эмулятор SIM-карточки на куске текстолита, но без каких либо проводов, идущих на компьютер. На этой плате устанавливается несколько микросхем: процессор Atmel AT89C51 (или AT89C52), внешнее ОЗУ на базе флэш-памяти, внешнее ППЗУ 64 Кб. Туда зашивается уже широко известная и готовая немецкая программа SIM_EMU.EXE (43 Кб). Может быть ее придется немного доработать. Питание на эту плату эмулятора подается, естественно, от телефона.

Сотовые системы-двойники

В России двойников имеют следующие сотовые и транковые системы:

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

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

Для создания двойника можно приспособить любой телефон, который может работать в системе, где работает телефон владельца. Для этого потребуется всего лишь разобраться в управляющей программе хост-процессора телефона.

Часть 6. Вопросы и ответы

Что такое сканирующий телефон?

Сканирующий телефон — это переделанная соответствующим образом трубка обычного радиотелефона. Чаще всего это Sanyo и Panasonic. Каждая модель телефона имеет несколько частотных каналов для работы. При установлении связи в обычном режиме трубка и база ищут свободный канал, затем обмениваются определенным кодом, соответствующим только этой паре трубка-база. База опознает свою трубку, подключается к телефонной линии, и вы говорите по телефону. Радиус действия современных бытовых радиотелефонов достигает около 500 м без дополнительных приспособлений. То есть можно звонить, находясь в соседнем доме, на улице, в автомобиле. Телефонный пират имеет трубку, которая сканирует частотные каналы и, обнаружив на каком-либо базу, начинает подбирать коды доступа. Базы не защищены от такого подбора, и один из кодов подходит. Трубка запоминает этот код в своей памяти. Теперь пират может звонить с этой базы, как со своего телефона, к примеру в Нью-Йорк. На домашнем телефоне хозяин легко может обнаружить пирата, заметив, что телефон работает «сам по себе». В случае, если же звонить с номера какой-либо фирмы в выходной день, вряд ли пирату помешают, пока не придет счет с МТТС.

Хочется заметить, что имея не очень навороченный «Панасоник» выпуска примерно 92–95 гг. без всякой переделки трубки можно просто проехать на машине или пройтись пешком по районам сосредоточения всевозможных офисов (такие районы есть в любом городе) и вашей трубке обязательно ответит чья-то база. Кодов-то всего у них 256, 512, максимум 1024. Один гражданин таким образом звонил с балкона своего дома через базу в офисе фирмы, расположенной поблизости.

Как защитить свой телефонный номер от сканирующих телефонов?

Владелец любого радиотелефона может стать жертвой радиопиратов. Чужие звонки в пределах города мешают, но денег не стоят. Материальный ущерб владельцу телефона наносят чужие междугородные и международные звонки. В случае, если вы редко звоните по межгороду, то можете попросить отключить на ГТС «восьмерку». В большинстве городов после этого вы вообще не сможете звонить по межгороду. В некоторых городах вы сможете заказать межгород и международку через дис-

петчера. При установлении связи диспетчер перезвонит вам и уточнит, действительно ли вы заказали этот разговор. Минусы: дольше дозваниваться и за услуги диспетчера вы платите дополнительно стоимость трех минут (в большинстве городов). Более удобный способ — приобрести на радиорынке или в радиомагазине устройство защиты телефона от пиратов. Оно смонтировано в корпусе обычной телефонной розетки и позволяет установить доступ к городской линии только после набора известного вам пароля из четырех цифр. Можно самостоятельно заблокировать «восьмерку». Хочется заметить, что я не согласен, что это устройство защищает плохо из-за того, что пароль можно подобрать простым перебором. Радиопират, трубка которого в плотном микрорайоне может выловить до 10–15 чужих баз, работает просто, как говорят воры, «на рывок». Не вышло с одной — уйдет к другой. А чтобы еще и доступ к линии подбирать... Совсем уж маньяком надо быть. Совсем крутым способом защиты является переделка базы.

Владельцы телефонов, подключенных к АТС с импульсным набором номера, могут переводить свой телефон в тоновый режим на то время, пока сами не звонят. Способ нехитрый, а помогает.

Где взять схему переговорного устройства по линии 220В?

Любители мастерить могут найти базовую схему на сайте http://www.logicnet. ru/~electron/. Там же есть множество других интересных схем. Можно заглянуть также на http://www.chat.ru/~nikbol/.

Сканируются ли радиотелефоны стандарта DECT?

В принципе — почему бы и нет? Раз уж DAMPC декодируют запросто. Но о том, что кто-то делает это на высоком уровне, пригодном для массового тиражирования, я не слышал. Аппараты стандарта DECT все-таки достаточно дороги и не очень широко распространены. Но я не говорю про «компетентные органы», у которых аппаратура декодирования появляется одновременно с появлением стандарта кодирования. Если не раньше.

Как бороться с помехами в телефонной сети? Существуют ли фильтры?

Однажды, в каком-то компьютерном журнале я видел рекламу девайсов под названием «Фильтр-усилитель телефонной линии» зарубежного производства. Стоил сей аппарат порядка 140 долларов и, якобы, усиливал сигнал в обе стороны и эффективно фильтровал от помех. Больше я подобной рекламы не встречал и живьем зверька не видел. Но вообще-то, усилить сигнал — это полдела и не столь большое достижение. А что касается помех (импульсных), то они имеют широчайший спектр, случайную негармоническую огибающую и прочие гадкие свойства. Отфильтровать активным фильтром такие помехи и не угробить полезный сигнал практически невозможно, если говорить о модемном сигнале. Глубоко влезать в теорию некогда, поверьте простой логике — если бы физическая фильтрация линии имела смысл, эти девайсы продавали бы на каждом углу, их бы засунули в чипы всевозможных модемов, а не доводили бы до невиданных высот программные методы фильтрации и коррекции.

А можно ли вообще в нашей стране звонить по межгороду/международке на халяву?

Да, можно. Используя несколько методов:

1. Звонить с чужого телефона (двойникового сотовика, панасотовика).

2. Использовать Russian GrayBox.

3.Использовать кульный девайс.

В случаях 1, 2 счет за телефонные переговоры приходит другому человеку.

В случае 3 можно поговорить с Америкой по цене звонка в Подмосковье.

Что такое «Russian GrayBox»?

Russian GrayBox — устройство для подмены номера по запросу АО междугородней АТС. На некоторых типах АТС возможно создать ситуацию, когда запрос АОН междугородней АТС попадает непосредственно на ваш абонентский комплект, а не блокируется станционной аппаратурой. Russian GrayBox эмулирует ответ вашей АТС и посылает ложный безинтервальный пакет с чужим номером, в этом случае АТС считает, что звонок по межгороду идет с другого номера (который подставлен в безинтервальном пакете) и счет за переговоры приходит на другой номер. Надо сказать, что Russian GrayBox работает только на старых типах АТС, найти их в крупных городах практически невозможно. Устройство Russian GrayBox существует как в переносимом, так и в упрощенном портативном варианте в виде бипера.

Что такое «кульный девайс»?

Кульный девайс — это фрикерский комплекс, позволяющий вести эксперименты с системой телефонной сигнализации на территории бывшего СССР. С помощью него можно, к примеру, позвонить по межгороду по очень низкой цене. Или попробовать подсоединиться к занятой линии.

Как сделать «кульный девайс»?

Сделать «кульный девайс» очень просто: надо взять любой модем, умеющий генерировать однотональные и двухтональные сигналы произвольной частоты, амплитуды и длительности в линию. Такими модемами являются, к примеру, модифицированный USR Sportster (или Russian Courier), модифицированный USR Courier, Digicomm Connection 14.4+ и другие. Затем нужно написать соответствующую управляющую программу на компьютере.

Какие системы сигнализации существуют на территории бывшего СССР?

В основном используются две системы, доступные для исследований: одночастотная и двухчастотная. Одночастотная система использует сигнал 2600 Hz и сигналы «2 из 6» для передачи контрольной информации и набора номера, двухчастотная система использует для этих целей различные комбинации частот 1200 и 1600 Hz.

Система двухчастотной сигнализации является более старой и в настоящее время используется все реже. Определить тип сигнализации, используемой в междугороднем канале, можно на слух: если при соединении или разъединении слышен однотональный сигнал, то используется одночастотная система, если слышен характерный двухтональный сигнал — используется система 1200/1600.

Какие сотовые телефоны ломаются?

Ломаются любые телефоны, если их сбросить с десятого этажа на асфальт.

Какие сотовые системы имеют двойников и какие сотовые телефоны можно приспособить для создания двойника?

В России двойников имеют следующие сотовые и транковые системы:

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

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

Для создания двойника можно приспособить любой телефон, который может работать в системе, где работает телефон владельца. Для этого потребуется всего лишь разобраться в управляющей программе хост-процессора телефона.

Какие процессоры используются в сотовых телефонах?

Это зависит от модели телефона и фирмы-производителя. Вот примерный список:

- Motorola Хост: 68HC11, DSP: AT&T16XX, MC566XX
- Ericsson Хост: ARM7TDMI core, DSP: Texas Instruments
- Nokia Хост: H8/XXX, Z80

Я нашел на улице отключенный сотовый телефон. Как бы сделать так, чтобы по нему бесплатно можно было звонить?

Это сделать весьма непросто. Все зависит от модели телефона, протокола его работы, вида используемой в вашей местности сотовой связи и других параметров. В этом случае лучше обратиться к специалистам.

Где лучше прочитать про модификацию сотовых телефонов?

http://radiophone.dhp.com

Какие системы защиты от двойников существуют в сотовых сетях?

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

Что такое AKEY и как он работает?

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

На основе AKEY (постоянный ключ) с помощью хеш-функции CAVE, использующей в качестве входных параметров, помимо AKEY, ESN, MIN телефона, а также случайное число, присланное по эфиру с базовой станции, генерируется временный ключ, называемый SSD_A (тоже 8 байт). Этот ключ в дальнейшем и используется при аутентификации для генерации ответного значения. Постоянный AKEY не используется при аутентификации и служит только для расчета временного ключа. При установлении соединения система передает сотовому телефону

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

Периодически (примерно раз в неделю) станция посылает сотовому телефону сообщения о генерации нового временного ключа, SSD_A, по получении этого сообщения (SSD_UPDATE) телефон рассчитывает новый временный ключ SSD_A, используя уже известный постоянный AKEY, ESN, MIN и случайное число со станции. В итоге, сам ключ аутентификации (SSD_A) является временным и периодически меняется, и становится бессмысленным «клонирование» трубок (а также нахождение SSD_A методом последовательного перебора), поскольку после первого же изменения ключа работать дальше будет только один телефон с новым ключом.

Нельзя ли расшифровать АКод по посылкам со станции и ответам трубки?

Это можно сделать только методом прямого перебора кодов, да и то с ограничениями. Функция CAVE является односторонний хеш-функцией с маленькой разрядностью выходного кода, поэтому вычислить ключ по данным, передаваемым по эфиру практически невозможно.

Что такое SIS и как он работает?

SIS (Subscriber Identity Security) — система аутентификации и защиты информации пользователей сотовой сети NMT-450i.

Принцип действия SIS аналогичен AKEY: при запросе на соединение станция посылает сотовому телефону случайное число, которое обрабатывается хеш-функцией SIS в телефоне с использованием 120-битового уникального ключа пользователя, часть результата хеш-функции посылается на базовую станцию для сравнения, другая часть используется для шифрования набираемого номера.

В отличие от AKEY, SIS не меняется и всегда остается постоянным для конкретного телефона, а также обеспечивает шифрование набираемого номера (в системе AKEY тоже предусмотрена возможность шифрования номера, однако она не используется в российских системах).

Также, в отличие от AKEY, SIS-код зашивается в телефон производителем и не может быть изменен провайдером услуг (AKEY обычно может вводиться с клавиатуры).

Как смотреть НТВ+ и другие каналы, кодированные в системе Nagravision-Syster, если нет возможности смотреть их официально?

Спутниковое телевидение существует как бесплатное, так и коммерческое, для просмотра которого надо платить телекомпании абонентскую плату. Для того чтобы обеспечить сбор абонентской платы, телекомпании кодируют свой сигнал, то есть делают невозможным просмотр его без специального декодера. Телекомпания НТВ+ использует Французскую систему кодирования Nagravision-Syster, в которой используется перемешивание строк по особому алгоритму, в соответствии с таблицей перестановки строк. Кроме того, применяется инверсия спектра звукового сопровождения частой 12,8 кГц, что очень сильно искажает звук, делая невозможным его прослушивание. Вдобавок ко всему, для разграничения доступа оплативших и не оплативших подписку абонентов, применяется система адресного кодирования — то есть телекомпания имеет возможность сигналом со спутника избирательно выключать декодеры не оплативших абонентов. Достигается это тем, что у подписчиков имеются индивидуальные ключи, представляющие собой микросхему памяти, в которой содержится индивидуальный код, а также обновляемая через спутник информация о состоянии подписки. Эту же систему кодирования применяют телекомпании Германии, Франции, Польши, а также ряда других стран. Не смотря на то, что этой системе уже более десяти лет, протокол обмена данными между ключом и декодером телевизионными пиратами изучен мало (наверное, просто это было никому не нужно), о работающих эмуляторах ключей пока не слышно.

Система кодирования Nagravision-Syster была взломана другим способом — появились пиратские декодеры, которые работают безо всяких ключей на принципе подбора кода путем сравнения и поиска похожих строк. Такие декодеры открывают все каналы, на которые они рассчитаны и совершенно бесплатно. К сожалению, купить такой декодер у нас пока невозможно, а сделать тоже очень сложно в основном из-за отсутствия необходимой информации.

Но недавно появилась возможность смотреть НТВ+ и другие каналы кодированные в Nagravision-Syster с помощью персонального компьютера, используя тот же принцип, что и у пиратского декодера, но реализуя его с помощью специальной программы. Этот способ получил общее название PC-TV. PC-TV позволяет смотреть все каналы, кодированные в Nagravision.

Для просмотра кодированных каналов таким способом, во-первых, нужен настроенный комплект спутникового телевидения, состоящий как минимум из антенны (тарелки), конвертера и ресивера. Эта система должна обеспечивать уверенный прием тех кодированных каналов, которые вы хотите смотреть. Для случая с НТВ+ достаточно иметь родной «НТВшный» комплект с «тарелкой» того диаметра, который достаточен для приема сигнала в вашей местности, можно без оригинального декодера.

Во-вторых, нужен достаточно мощный IBM совместимый персональный компьютер, минимум — P-166MMX, 32 Mb RAM, видеоадаптер PCI 4Mb, желательно P-II с как можно большей тактовой частотой и оперативной памятью 64 Mb. Объем и скорость жесткого диска, а также другие параметры, существенно не влияют.

В-третьих, для ввода изображения в компьютер, нужна карта видеовхода, построенная на одном из следующих чипов — BT848, BT849, BT878, BT879. Сейчас таких карт выпускается достаточно много, разными фирмами, под разными названиями, например: MiroPCTV, AverMedia различных модификаций, Fly Video (наверное, самый дешевый вариант), MR Vision TV Link, ТЕЛЕМАСТЕР. Продолжать список можно еще, но нет смысла — подойдет любая карта, лишь бы она была сделана на чипе серии BT8XX. Карты отличаются друг от друга наличием и качеством встроенного TV тюнера для просмотра обычных эфирных телеканалов, наличием дистанционного управления тюнером, количеством видеовходов 1 или 2, качеством и удобством прилагаемого к ней софта и некоторыми другими наворотами, которые никаким образом не связаны с нашей задачей, так как в данном случае требуется только видеовход. В последнее время стали появляться версии программ для видеоадаптеров на чипе ATI с видеовходом (без BT8XX), но так как у меня такой карты нет, то я их не тестировал и ничего про них сказать не могу.

На сегодняшний день написано несколько программ — декодеров, которые совершенствовались их авторами (и не только авторами, потому что почти все они публиковались вместе с исходными текстами) и имеют каждая по несколько версий. У каждой программы есть свои достоинства и недостатки, и стоит попробовать их все, чтобы сделать для себя выбор. Лично мне более других понравилась MoreTV 3.10 — на мой взгляд, это наиболее удачная программа, которая позволяет смотреть каналы как в стандарте PAL, так и SECAM (НТВ+). У нее реализовано автоматическое включение-выключение декодирования при переходе от кодированных к некодированным каналам, прямое взаимодействие с картой видеоввода (достаточно установить драйвер карты, софт можно не ставить, программа сама настраивает карту), имеются удобные оперативные регулировки с помощью горячих клавиш, достаточно легка в настройке. К недостаткам

данной программы можно отнести не очень хорошую чистоту цвета в режиме SECAM (хотя у некоторых других программ при просмотре SECAM цвет вообще отсутствует) и интерфейс на немецком языке. Надо учесть, что для видеоадаптеров с видеовходом на чипе ATI, должна быть специальная версия программы — MoreATI-TV.

После того как вы установили карту видеовхода в ваш компьютер, надо соединить НЧ-вход карты с НЧ-выходом вашего ресивера с помощью специального низкочастотного кабеля, такого же, каким вы подключаете телевизор к ресиверу или видеомагнитофону. Установите драйвер и программное обеспечение карты, руководствуясь инструкцией, прилагаемой к ней.

В результате, если вы сделали все правильно, то при включенном ресивере и запущенной программе от карты, вы должны получить на экране компьютера устойчивое изображение того канала, на который настроен в данный момент ваш ресивер, в том виде, в каком оно передается со спутника (то есть если канал кодированный, то изображение будет напоминать фотографию). Не забудьте, что декодер в настройках ресивера должен быть выключен.

Теперь можно приступить к установке и настройке программы-декодера. Программы в основном не требуют инсталляции и достаточно просто распаковать архив в любую директорию, желательно в корневом каталоге вашего жесткого диска. В дальнейшем речь пойдет о настройках программы MoreTV 3.10 — если вы ее сумеете запустить, то и с остальными программами вы сумеете разобраться сами.

Первым делом скопируйте в каталог с программой файл Key.txt предназначенный для НТВ+, если вы настроили ресивер для его приема. Учтите, что Key.txt для НТВ+ и для других каналов разные! Не забудьте переименовать файл Key2.txt (извлеченный из архива) в Key.txt (без цифры) и запустите программу.

На экране появится окно настроек программы. В рамке «**Video**» установите для начала разрешение 640x480YUY2 и поставьте флажок **SECAM**. В рамке «**Hardware**» выберите из списка вашу карту (если ее нет в списке, сильно не расстраивайтесь, выберите любую другую, лишь бы на таком же чипе, как у вас), марку тюнера можно не устанавливать — он нужен только при приеме кодированных каналов с эфирной антенны, PLL для начала лучше не включать. В рамке «**Dekodierung**» установите количество тестовых строк равным 30 и сохраните настройки (средняя кнопка). Теперь можно запускать собственно программу (верхняя кнопка).

Первый запуск программы может продлиться несколько дольше, чем обычно (в это время программа создает в своем каталоге индексный файл с именем **MoreTV_XX.idx**, где **XX** — количество тестовых строк), в дальнейшем программа будет запускаться практически мгновенно. Вы должны увидеть на экране декодированное изображение. В случае, если экран останется синим, проверьте все соединения, а если у вашей карты два входа, попробуйте подать сигнал на другой вход. В случае, если изображение есть, но не декодированное, проверьте, тот ли Key.txt вы используете (если открыть его блокнотом, он должен начинаться так: 0 1 2 3 4 5 6 7 2 5 4 7 8 9 10 11 14 17 16 19 22 25). В случае, если все заработало, попробуйте поэкспериментировать с настройками программы для достижения лучшего качества изображения.

«Горячие клавиши» программы: **Esc** — стоп кадр, **F1** — восстановление после стоп кадра, **F2** — включение декодера (включен/выключен/авто), **F3–F8** — изменение формата и размера декодируемого изображения, **F10** — выход из программы, **F11** — Турбо/стандартный декодер, **F12** — синхронизация по фазе, **Insert** — контрастность +, **Delet** — контрастность -, **Home —** насыщенность +, **End** — насыщенность -, **PgUp** — яркость +, **PgDn** — яркость -, остальные клавиши предназначены для настройки и переключения каналов встроенного TV тюнера и для нас значения не имеют.

Программа MoreTV не имеет встроенного декодера звука. На сегодняшний день есть три способа прослушивания звукового сопровождения. Способ первый, самый простой и самый худший. Скачайте одну из программ — аудио-декодеров (лично мне больше нравится DCPlus), соедините выход звука ресивера с линейным входом звуковой карты вашего компьютера, в настройках стандартного регулятора громкости Windows включите линейный вход на запись, и обязательно выключите на воспроизведении (чтобы предотвратить проникновение кодированного звука непосредственно со входа на выход без обработки программой). Запустите программу с установками по умолчанию, и звук должен заработать. Качество звука регулируется настройками программы. Не забудьте, что для этого ваша звуковая карта обязательно должна поддерживать Full Duplex — то есть одновременную запись и воспроизведение звука, и эта опция должна быть активизирована в настройках звуковой карты (установить флажок «разрешить двунаправленную работу»). Кроме того, одновременная работа программ аудио- и видеодекодеров возможна только на достаточно быстрых машинах, а если конфигурация вашего компьютера соответствует только минимальным требованиям, то этот способ для вас непригоден (в зависимости от используемой программы и ее настройки будет «заикаться» звук либо срываться картинка).

Второй способ подойдет тем, у кого есть оригинальный декодер с неоплаченным ключом и кто не боится держать в руках паяльник. Аккуратно вскройте декодер, найдите микросхему с надписью EURO@DEC 5096 ELEXC7397A. Отпаяйте сопротивление от седьмой ноги микросхемы и подайте на эту ногу микросхемы логическую единицу (+5 В) через сопротивление 1–10 к (найдите напряжение +5 В с помощью тестера по цепям питания). Соблюдайте осторожность, так как на плате декодера присутствует высокое напряжение!!! Ошибка в ваших действиях может привести к серьезной поломке декодера!!! После этой переделки декодер открывает звук и без оплаты. Третий способ годится для опытных радиолюбителей. Соберите самодельный декодер по приведенной схеме. Этот способ наиболее сложен, но наверно самый лучший, так как не требует наличия оригинального декодера, не занимает ресурсы компьютера, звук не запаздывает по отношению к видео, как в программных декодерах.

После того, как у вас все получилось, возможно вам захочется вывести изображение на телевизор. Для этого ваш видеоадаптер должен иметь TV-OUT. Практически все современные модели видеоадаптеров имеют модификации с выходом на телевизор. Это видеоадаптеры на таких чипах как: RIVA TNT, RIVA 128, ATI, INTEL 740, S3 VIRGE GX2, а также некоторые другие. Телевизор подключается к выходу видеоадаптера (чаще всего это обычный «тюльпан») кабелем, аналогичным тому, которым вы подавали сигнал на вход карты видеовхода. Настраивается адаптер в соответствии с руководством пользователя, прилагаемого к нему. Надо заметить, что практически все видеоадаптеры «усекают» или «поджимают» изображение по вертикали примерно на 5–10%. Это связано с несоответствием количества строк в телевизионном стандарте и изображении, формируемом видеоадаптером. Существуют специальные дополнительные карты — TVOUT, которые преобразуют стандартное SVGA изображение, формируемое любым видеоадаптером, в полноценный сигнал формата PAL, но я встречал о них информацию только в Интернет и пока не разу не видел их в продаже.

Часто задают вопрос — часто ли телекомпании меняют код, и отличается ли он на разных каналах одного пакета программ? Здесь можно пояснить, что программные декодеры не требуют никаких кодов, они их подбирают «на ходу» методом сравнения соседних строк. В алгоритме декодирования используется только таблица перестановки строк (файл Key.txt) одна для всех каналов НТВ+. В оригинальных декодерах эта таблица содержится в программе-прошивке центрального процессора, то есть программируется однократно при изготовлении декодера. Соответственно сменить эту таблицу можно, только заменив все декодеры у официальных подписчиков.

Иногда задают вопрос — можно ли все-таки сделать аппаратный декодер, то есть обойтись без компьютера? В принципе это возможно, на сайте www.eurosat.com/salp описан декодер, декодирующий все французские каналы. Так как PC TV с ключом Key.txt, подходящим для НТВ+, открывает французские каналы, логично предположить, что данный аппаратный декодер будет открывать и НТВ+, однако я не знаю случаев, чтобы это кто-то проверил на практике. Изготовление данного декодера технологически сложно и может обойтись не в одну сотню долларов, а также нет никакой гарантии успеха этого предприятия, и поэтому на сегодняшний день наиболее простым способом просмотра каналов кодированных в Nagravision является PC TV.

Приложения

Словарь сокращений в области телефонной связи

2ВСК

2 выделенных сигнальных канала

STP

Транзитный пункт сигнализации

АВУ

Абонентская высокочастотная установка

АВУ ВЧ

Абонентская высокочастотная установка, высокочастотная часть

АВУ НЧ

Абонентская высокочастотная установка, низкочастотная часть

АЛ

Абонентская линия.

АМТС

Автоматическая междугородная телефонная станция.

АОН

Автоматическое определение номера

АТСДШ

Автоматическая телефонная станция декадно-шаговая.

АТСК

Автоматическая телефонная станция координатная.

АТСКЭ

Автоматическая телефонная станция квазиэлектронная.

АТСЭ

Автоматическая телефонная станция электронной системы коммутации

ЗСЛ

Заказная соединительная линия.

ИКМ

Импульсно-кодовая модуляция (способ кодирования аналогового сигнала)

ИКМ-30/32

32-канальная цифровая система передачи (30 разговорных трактов)

МЦК

Междугородный центр коммутации

ОПС

Опорная станция.

ОПТ

Опорно-транзитная телефонная станция.

ПС

Пункт сигнализации

ПС

Подстанция.

СЛ

Соединительная линия.

СЛМ

Соединительная линия междугородная.

ТС

Транзитная станция.

УАК

Узел автоматической коммутации

УВС

Узел входящих сообщений

УВСК

Узел входящих сообщений координатный

УВСМ

Узел входящей связи междугородний

УВСШ

Узел входящих сообщений декадно-шаговый

УВСЭ

Узел входящих сообщений электронный

УВТС

Узел ведомственных телефонных станций

УИВС

Узел исходящих и входящих сообщений

УИВСЭ

Узел исходящих и входящих сообщений электронный

УИС

Узел исходящих сообщений

УИСК

Узел исходящих сообщений координатный

УИСЭ

Узел исходящих сообщений злектронный

УИСЭ-0

Узел исходящей связи для «0» направления.

УПАТС

Учрежденческо-производственная автоматическая телефонная станция.

УПСГ

Узел пригородно-сельской связи городской

УСПМ

Узел смешивания потоков междугородний

УСС

Узел спецслужб

УССЭ

Узел специальных служб электронный

Список использованных материалов

Фрикинг и его последствия

Pikachu Pokemon

Фрикеры, хакеры, МГТС... Отключайся!

Игорь Ветров

Клонирование терминалов сотовой связи

Ольга Мобильная

Мошенничество с телефонными картами

http://www.osp.ru

Шпионы — радиолюбители

Сергей Чертопруд

Перехват трафика

О.Н. Перетятко

Краткая хроника истории органов и войск правительственной связи

http://www.obereg.ru

Флай

Алекстандр Игорев

Принципы построения и функционирования проводных систем связи и коммутации, а так же их основных узлов.

Сергей Качашкин

Эксплуатация и ремонт абонентских устройств городских телефонных сетей

Г.А.Зуев, Л.И.Хачиров

Модемы: ЧТО ДЕЛАТЬ и КТО ВИНОВАТ?

Игорь Дианов

Одновременная передача голоса и данных через канал тональной частоты

Мухин С.В.

Телефония. Теория и техника передачи речи

Покровский Н.Б.

Голос через IP звучит все лучше
Тим Грин

Как налить море в наперсток? Технологии компрессии голоса
Александр Крейнес

Блюзы говорящих модемов
Барри Филипс

История развития протоколов передачи данных
Мухин С.В

Кабельные Модемы
Кунегин С. В.

Список использованных источников:

http://www.kunegin.narod.ru/

http://www.xdsl.ru/

http://www.ccc.ru/

http://www.osp.ru/

http://www.itu.int/

http://www.adsl.com/

http://www.emap.com/cwi/

http://www.zdnet.com/intweek/

http://www.teledotcom.com

http://www.internettelephony.com

Содержание

Введение

Часть 1. Классификация

Часть 2. Боксинг

Часть 3. Модемы и IP-телефония

Часть 4. Собери свой жучок

Часть 5. Тонкости, хитрости и секреты

Часть 6. Вопросы и ответы

Приложения

Научно-популярное издание

Леонтьев Борис Константинович

Как ломают телефонные сети

Пособие по взлому и защите телефонных сетей

Главный редактор *Б. К. Леонтьев*
Компьютерная верстка *И. В. Царик*

Подписано в печать 30.04.2006. Формат 60x90/16.
Гарнитура «Ньютон». Бумага офсетная. Печать офсетная.
Печ. л. 20. Тираж 3000.

ООО «Литературное агентство «Бук-Пресс».
127591, Москва, Керамический пр., д. 53. кор. 1.
http://www.book-press.ru.