УДК 681.3.

Стишенко И.К.

Общие принципы промышленного шпионажа на линиях связи

МЕТОДЫ И СРЕДСТВА НЕСАНКЦИОНИРОВАННОГО ПОЛУЧЕНИЯ ИНФОРМАЦИИ В ПРОВОДНЫХ КАНАЛАХ СВЯЗИ

Зоны подключения

С точки зрения промышленного шпионажа существуют потенциальные возможности перехвата речевой информации, передаваемой по проводным телефонным линиям. Рассмотрим перехват информации, основываясь на типовой телефонной системе связи, которая представлена на рис. 1. На рисунке в качестве коммутаторов представлены цифровые АТС.

Условно телефонный канал можно разбить на участки – зоны НПИ. Согласно рисунку к зоне А относится телефонный аппарат. Сигнал с телефонного аппарата поступает на распределительную коробку – в зону Б, далее поступает по абонентскому кабелю на распределительный щит (зона В) и затем по линейному кабелю – на кроссовое оборудование АТС (зона Г). На станции с кроссового оборудования групповой телефонный сигнал поступает на промщит, предназначенный для внутристанционных коммутаций (зона Д), а затем на абонентский комплект оконечной АТС. Между АТС организованы соединительные линии, которые образуют зоны Е, Ж, З и И. В зонах Е и Ж в основном передается городской трафик, в зоне З – междугородний, а в зоне И – международный трафик.

Рассмотрим, что из себя представляют указанные зоны. Зона А включает в себя телефонный аппарат. Вопросы перехвата сигналов отражены в специальной и популярной литературе. Зона Б включает в себя участок абонентской линии от телефонного аппарата до распределительной коробки, а также саму коробку. Обслуживание абонентской линии выполняется телефонистами и большей своей части проходит по помещениям абонентов. Распределительная коробка, как правило, находится снаружи помещений абонентов. Контроль состояния коробок осуществляется в основном при проведении работ на линиях по заявке абонентов. Длина зоны составляет до нескольких десятков метров.

Зона В включает в себя участок кабеля от распределительной коробки до распределительного шкафа и сам шкаф. Это, как правило, 10-20 парный кабель, который находится в обслуживании монтеров АТС. Распределительный шкаф, как правило, находится в легко доступных местах (открытые подвальные помещения либо непосредственно возле стен зданий). Длина зоны составляет до нескольких единиц километров.

Зона Г включает в себя участок кабеля от распределительного шкафа до станционного кабеля и включает в себя ряд соединительных муфт. Используется многопарный кабель от 100 пар и выше. Кабель укладывается в кабельную канализацию. Большое количество пар затрудняет перехват информации в конкретной паре.

Зона Д включает в себя межстанционные кабели на оконечной станции и кроссовое оборудование. Емкость этого кабеля варьируется в широких пределах. Кабель находится в хорошо контролируемых помещениях с ограниченным кругом лиц, имеющих доступ к этому участку. На кроссовом оборудовании кабель и каждая пара маркируются. Маркировка пары может быть выполнена до последних цифр телефона абонента.

Зона Е включает в себя межстанционные соединительные линии. Требования к характеристикам кабеля соответствуют требованиям участка Г. При большом объеме трафика применяется кабель, обеспечивающий работу систем с уплотнением каналов (цифровые и аналоговые системы). В качестве среды передачи применяются как металлические, так и волоконно-оптические кабели. В этой зоне распределение соединений

по линиям происходит в динамическом режиме, т.е. вызов на один и тот же номер может пройти в разное время по разным соединительным линиям.

В зонах Ж, З и И как правило, используется кабель, обеспечивающий работу ЦСП. Зона Ж может иметь значительную протяженность, в то время как зона З имеет ограниченную протяженность. Как правило, зона З находится внутри контролируемого помещения с ограниченным кругом лиц, имеющих доступ к этому участку. В этих зонах распределение соединений по каналам систем передач происходит в динамическом режиме. На участке Ж в основном используется волоконно-оптический кабель и ЦСП PDH и SDH иерархии. Эти зоны могут находиться в обслуживании у операторов, предоставляющих услуги передачи информации (операторы первичных сетей связи).

Зона И представляет собой стык первичных и вторичных сетей и строится на основе систем передачи высокой пропускной способности на базе первичных сетей ВОЛС. В связи с большими объемами передаваемой информации в первичных сетях перехват конкретного вызова сопряжен с большими материальными и техническими трудностями. Зона И предполагает организацию международного перехода на первичные сети связи операторов других стран.

Методы и способы несанкционированного получения информации

Наиболее распространенными методами и способами перехвата телефонных переговоров являются:

1. непосредственное (контактное) подключение;
2. подключение бесконтактным методом;
3. метод использования радиозакладок;
4. перехват побочных электромагнитных сигналов и наводок (ПЭМИН);
5. стационарное прослушивание телефонных переговоров на телефонной станции

Непосредственное подключение является наиболее простым и распространенным способом. Для негосударственных организаций, которые занимаются промышленным шпионажем, наиболее доступными являются зоны подключения А, Б, В и Г. Способы выполнения непосредственного подключения – установка стационарного параллельного телефона, временное подключение с помощью стандартного тестового телефона («монтерской» трубки) в любом месте абонентской проводки, подключение к воздушной линии, подключение к линии связи через согласующее устройство и с использованием устройства компенсации падения напряжения. Общим недостатком всех способом контактного подключения является необходимость нарушения целостности проводов и непосредственное влияние устройств перехвата на характеристики линий связи.

Бесконтактный метод устраняет отмеченные недостатки контактного метода. Способы выполнения метода – подключение через индуктивный датчик (согласующий трансформатор) или датчик, основанный на эффекте Холла. Выпускается большое количество датчиков, интегрированных вместе с диктофонами. Работа таких систем основана на включении записи при появлении сигнала в линии связи. Основным недостатком метода является необходимость иметь постоянный доступ в помещение для замены магнитных носителей информации.

Метод использования радиозакладок устраняет необходимость постоянного доступа в помещение, т.к. перехваченная информация передается по радиоканалу на регистрирующее устройство. Для повышения скрытности работы радиоканала применяется

шифрация сигнала и используются нетрадиционные виды модуляции передаваемого сигнала. Для увеличения дальности передачи сигналов используют ретрансляторы.

Перехват телефонных переговоров на основе ПЭМИН основан том, что любое электронное устройство при работе создает электромагнитное излучение. Способы выполнения метода – прокладка параллельных проводке проводов, способы акустического прослушивания помещений (телефонный аппарат содержит систему передачи речевой информации, используются конструктивные недостатки стационарных телефонов, используется высокочастотное навязывание).

Перехват информации с многоканальных кабельных и волоконно-оптических линий связи и выделение телефонных разговоров интересующих абонентов представляет собой весьма сложную задачу. Доступ к коаксиальным кабелям затруднен, т.к. они прокладываются в специальных кабельных канализациях. При этом кабели заключены в герметическую оболочку, которая в свою очередь находится под давлением. Нарушение целостности оболочки приводит к падению давления и срабатыванию тревожной сигнализации. На вооружении спецслужб находится универсальная аппаратура, которая применяется для съема информации с любых кабельных линий связи. Примером такого оборудования может служить американская система «Крот». Такие системы были установлены во многих странах, включая Россию.

Проведение перехвата информации с подводных линий связи представляет собой сложное и дорогостоящее мероприятие. Однако для его осуществления также разработана соответствующая аппаратура, которая стоит на вооружении спецслужб. Примером такого оборудования может служить американская система «Камбала».

Возможности и принцип работы таких разведывательных систем более подробно описаны в [1].

Таким образом, в настоящее время имеется целый арсенал средств разведки, предназначенных для перехвата информации с кабельных линий связи: для симметричных ВЧ-кабелей разработаны устройства с индуктивными датчиками, для коаксиальных и НЧ-кабелей – устройства с возможностью непосредственного подключения и отвода минимальной части энергии для осуществления перехвата информации. Для специальных кабелей, внутри которых поддерживается постоянное давление воздуха, применяются устройства, компенсирующие его снижение при подключении, в результате чего предотвращается срабатывание аварийной сигнализации. Учитывая, что перехват информации непосредственно с коммутационных систем связи операторов иностранных государств крайне затруднен, а порой и невыполним, использование таких систем перехвата оправдано по отношению к линиям связи операторов.

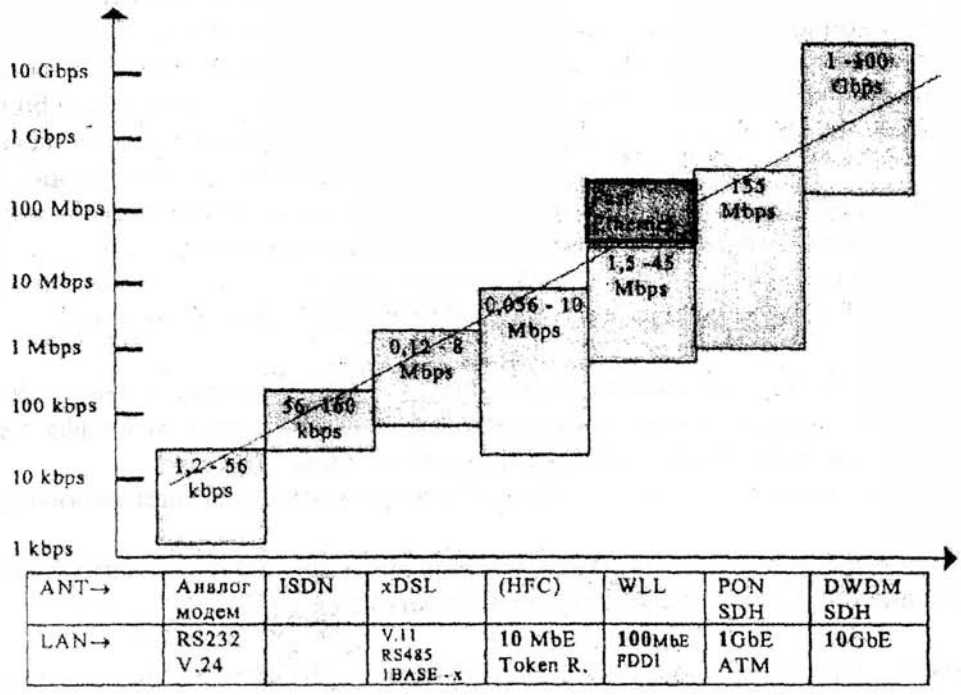
Рассмотренные зоны перехвата относятся к перехвату информации с линейно-кабельных сооружений. Вместе с тем существуют и реализованы способы перехвата вызовов, используя ресурсы коммутационных систем. Принцип перехвата состоит в следующем. Интересующий телефонный номер заносится в коммутатор. При поступлении входящего или исходящего вызова на указанный телефонный номер коммутатор организует дополнительную связь со специальным оборудованием. Дополнительное соединение не оказывает влияния на качество осуществляемого соединения при этом абонент продолжает получать полный комплекс заказанных услуг связи. У большинства коммутационных систем (5ESS Lucent Technologies, Siemens, 1000E10 Alcatel, AXE-10 Ericsson и т.д.) существует возможность организации ограниченного контроля соединений абонентов. Данная функция используется оператором по заявке абонента при ухудшении качества предоставляемых услуг связи. Эту же функцию можно использовать и для организации перехвата информации, проходящей через коммутационную станцию. Кроме того, в состав коммутационных станций могут дополнительно вводиться специальные аппаратно-программные средства, позволяющие проводить перехват информации по заранее указанным абонентам. Управление перехватом может осуществляться из удаленного пункта управления. Так,

согласно «Совместному решению по эксплуатационно-техническим требованиям к средствам и сетям электросвязи для обеспечения оперативно-розыскных мероприятий», которое действует на территории России, предусматривается возможность по командам из пункта управления изменять состав услуг на заданный период времени и осуществлять подключение линий службы безопасности к любым абонентским линиям, в том числе уже находящимся в состоянии соединения. При этом со специального оборудования снимается информационная и сигнализационная части перехватываемого соединения. Это устройство обеспечивает полную развязку соединений. Подобное оборудование применяется правоохранительными органами, однако существует возможность использования данного ресурса коммутационной станции для организации несанкционированного получения информации персоналом АТС. Выявить использование данного ресурса коммутатора с технической точки зрения крайне трудно.

Понятие коэффициента эффективности перехвата.

За последнее время наблюдается тенденция интеграции транспортных сетей от абонента до абонента. Это обусловлено следующими причинами.

1. Наблюдается «выравнивание» пропускной способности или производительности этих участков сети [7]. Можно ожидать, что будущее развитие местных сетей будет происходить по правилам, диктуемым локальными вычислительными сетями.



ANT→	Аналог модем	ISDN	xDSL	(HFC)	WLL	PON SDH	DWDM SDH
LAN→	RS232 V.24		V.11 RS485 10BASE - x	10 MbE Token R.	100MbE FDDI	1GbE ATM	10GbE

Рис. №2. Динамика роста пропускной способности в транспортных сетях доступа

2. Стоимость оборудования систем передачи уменьшается как в пересчете на канал, так и в абсолютных показателях, т. е. стоимость оборудования почти не зависит от числа каналов.

3. Оборудование на различных участках сети (абонентском, местном, зоновом, магистральном) становится однотипным (унифицированным).

4. Постепенное развитие телефонной плотности, рост числа услуг и увеличение неречевых информационных объемом привели к ощутимому изменению распределения трафика на различных участках сети. Происходит выравнивание

трафика на всех участках сети, другими словами интенсивность нагрузки на участке доступа и магистральном участке первичной сети выравниваются.

С другой стороны, стало ясно, что почти не претерпевшие изменений сети доступа стали сдерживать возможность получения широкого спектра информации, т. е. получения телекоммуникационных услуг.

Основной недостаток традиционных абонентских сетей доступа заключается в том, что они накладывают ограничение на организацию услуг и служб связи, которые используют широкополосный двунаправленный режим обмена информации, к которым относятся видеотелефония, видеоконференция, цифровое кабельное телевидение с использованием алгоритмов сжатия изображения типа MPEG, интерактивное телевидение и «закрытые» видеоканалы, подключение к сети Internet и серверам предоставления интеллектуальных услуг по скоростным каналам связи и т.д.

Реорганизация абонентского доступа на основе использования волоконно-оптического кабеля

В связи с тем, что в последнее время отмечается значительная потребность в передаче широкополосных сигналов, происходит освоение более высокочастотного диапазона электромагнитных волн. При этом осваиваются диапазоны миллиметровых и оптических волн для организации систем связи. Это приводит к тому, что все шире используются волоконно-оптических кабелей при создании линий связи. По некоторым данным в 90-х годах 20 века волоконно-оптические линии связи составляли порядка 10 % от общего количества их количества. В дальнейшем предполагается подавляющее большинство вновь строящихся линий связи создавать на основе волоконно-оптического кабеля. Происходит техническая революция в смене носителей информационного сигнала.

Развитие абонентских сетей доступа проходит по следующим концепциям:

- концепция «волокно в монтажный шкаф» FTTC (fiber to the curb);
- концепция «волокно в квартиру» FTTH (fiber to the home);
- концепция гибридной волоконно-коаксиальной сети HFC (hybrid fiber/coax).

В FTTC волоконно-оптический кабель из центрального узла (оконечной АТС или узла оператора услуг связи) приходит в монтажный шкаф. На участке от шкафа к абонентам применяются имеющиеся или вновь проложенные витые пары.

В FTTH волоконно-оптический кабель от центрального узла идет непосредственно в квартиру абонента.

HFC предназначена для оказания дополнительных услуг на базе коаксиальных телевизионных каналах. Схема построения сети аналогична FTTC.

Широкое использование волоконно-оптических кабелей в транспортных сетях доступа приводит к изменению методов и способов перехвата информации. В связи с этим специальные системы разведки, разработанные в более ранний период, не способны осуществлять перехват информации на линиях связи, построенных на транспортных сетях передачи информации.

Принято считать, что использование оптических волокон в качестве физической среды передачи информации по сравнению с существующими электрическими кабелями в плане обеспечения защиты информации предпочтительно по следующим причинам:

- высокая устойчивость к воздействию окружающей среды и электромагнитным помехам;
- гальваническая развязка по питанию различных элементов сети;

- отсутствие излучений и наводок на соседние информационные каналы, линии и устройства;
- сложность несанкционированного получения информации.

Сутью несанкционированного получения информации с оптического волокна является использование существующих или создание неоднородностей, на которых происходит рассеяние части оптического сигнала. Эта часть оптической энергии принимается приемником оптического сигнала и осуществляется перехват информации.

Самым ярким примером создания неоднородностей является сварка волокон, которая осуществляется периодически по длине линии связи через строительные длины оптического кабеля. Другим источником излучения оптического сигнала является использование на линиях связи разъемных соединителей. В них часть оптической энергии излучается по следующим причинам:

- отсутствие полной радиальной согласованности стыкуемых волокон;
- отсутствие полной угловой согласованности осей световодов;
- наличие воздушных зазоров между торцами световодов;
- разницы в диаметрах световодов стыкуемых волокон.

По мнению специалистов ряда зарубежных фирм возможен перехват информации с волоконно-оптического кабеля. Как правило, рассматриваются способы перехвата излучаемой энергии в местах изгиба волокна.

В одном из них волокно зажимается между двумя пластинами, одна из которых имеет рифленую поверхность, предназначенную для деформации волокна. На другой пластине устанавливается фотоприемник и устройство регистрации информации.

В другом просто удаляют защитную оболочку волокна с помощью химических реактивов и изгибают волокно на определенный угол.

В третьем используется стеклянная трубка, заполненная жидкостью с высоким показателем преломления и с изогнутым концом. Трубка жестко фиксируется на оптическом кабеле, с которого предварительно снята оболочка. На противоположном конце трубки устанавливается объектив, который фокусирует световой поток и фотоприемник. С него электрический сигнал поступает на усилитель звукового сигнала и далее на регистрацию.

ЛИТЕРАТУРА

1. Ю.Ф. Каторгин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко «Большая энциклопедия промышленного шпионажа», СПб, Полигон, 2000 г.
2. Эволюция первичных (транспортных) сетей. Часть 1,2 и 3 / Бирюков Н.Л. //.Вестник УБЕНТЗ. -1999. - № 8. - С. 5-12; 2000. - № 1. - С. 7-11; 2001. - № 1. - С. 8-13. [www.undiz.kiev.ua, email: nlbir@undiz.kiev.ua]

Поступила 23.05.2002