Побочное электромагнитное излучение и наводки (ПЭМИН) линий связи.

Эссе подготовил студент 017 гр. Царский А.Е.

Вступление.

Одним из наиболее вероятных каналов утечки информации в компьютерных сетях считается побочное электромагнитное излучение и наводки (ПЭМИН), создаваемые техническими средствами, то есть персональными компьютерами и линиями связи. Так как ПЭМИН канал способен переносить сигнал на расстояния в десятки и сотни метров. Наиболее мощными источниками ПЭМИН в ПК являются дисплеи, дисководы и принтеры. Протяженные проводные линии связи также создают сильные электромагнитные поля в окружающем пространстве, в особенности современные высокоскоростные компьютерные сети. Несмотря на многочисленные исследования по разработке и усовершенствованию оборудования, для уменьшения ПЭМИН от линий связи, защита от перехвата данных в проводах LAN остается большой проблемой.

В данной работе рассматривается опасность перехвата информации за счет излучения именно линий связи и наводок, создаваемых в линиях электропитания и заземления. Также приведены результаты исследований западноевропейской тестовой лаборатории по защищенности некоторых типов сетевых кабелей от побочных излучений.

Условия существования возможности перехвата информации.

Наличие сигналов ПЭМИН за пределами территории учреждения (ТУ) дает возможность перехватить их, тем самым создает канал утечки данных. ТУ в данном случае называется территория контролируемая учреждением, на которой исключено нахождение посторонних лиц и специальной подслушивающей аппаратуры. Средой распространения сигналов являются не только воздух и телефонные линии связи, но и линии электропитания, пожарной сигнализации, а также коммуникации (в том числе трубы водоснабжения и отопления) выходящие за ТУ.

Вероятность утечки информации по ПЭМИН каналу зависит от таких факторов, как:

- мощность источника излучения;
- характеристики среды распространения (ослабление и искажение сигнала в среде);
- характеристики принимающей аппаратуры.

Основной характеристикой канала, зависящей от выше перечисленных факторов, является отношение информативный сигнал/шум на входе приемника. Чем ближе приемник расположен к источнику сигнала, тем больше это отношение, тем более вероятно правильное распознавание сигнала.

При разработке системы мер по защите информации следует исходить из предположения, что принимающая аппаратура может быть установлена в любой точке вне ТУ, вплоть до ее границ.

Следовательно, если ПЭМИН сигнал может быть принят вне ТУ, то считают, что данный канал утечки информации существует.

Защищенность кабельных сетей от перехвата данных.

Проблема ПЭМИН для LAN чрезвычайно важна. В современных компьютерных сетях наиболее распространены кабели на основе витых пар. Они разработаны для передачи сигнала в «симметричном режиме», при этом предполагается, что токи, текущие по проводам витой пары навстречу друг другу, равны по величине. В таком случае побочное излучение отсутствует. Из-за недостижимости идеального режима на практике, ввиду невозможности произвести «идеальный» кабель и нагрузок, создаваемых при работе активного оборудования, в кабеле всегда присутствует неравенство токов. То есть имеет место «несимметричный режим». Излучения обоих проводов складываются, в результате происходит значительное излучение от витой пары.

Швейцарская лаборатория Data Security at Montena emc SA исследовала некоторые из наиболее распространенных в LAN типов кабелей, с целью выяснить защищенность от перехвата данных в сетях, использующих эти кабели.

Измерения степени риска перехвата проводились на реальной сети, так как теоретическая оценка учитывает множество факторов и слишком сложна. В эксперименте использовались три стандартных метода обнаружения информативных сигналов для различных протоколов передачи:

- измерение паразитной составляющей «несимметричного режима» с помощью токового датчика;
- измерение напряжения, которое наводится на согласованной параллельной силовой линии;

- измерение мощности излученной электромагнитной волны с помощью антенны.

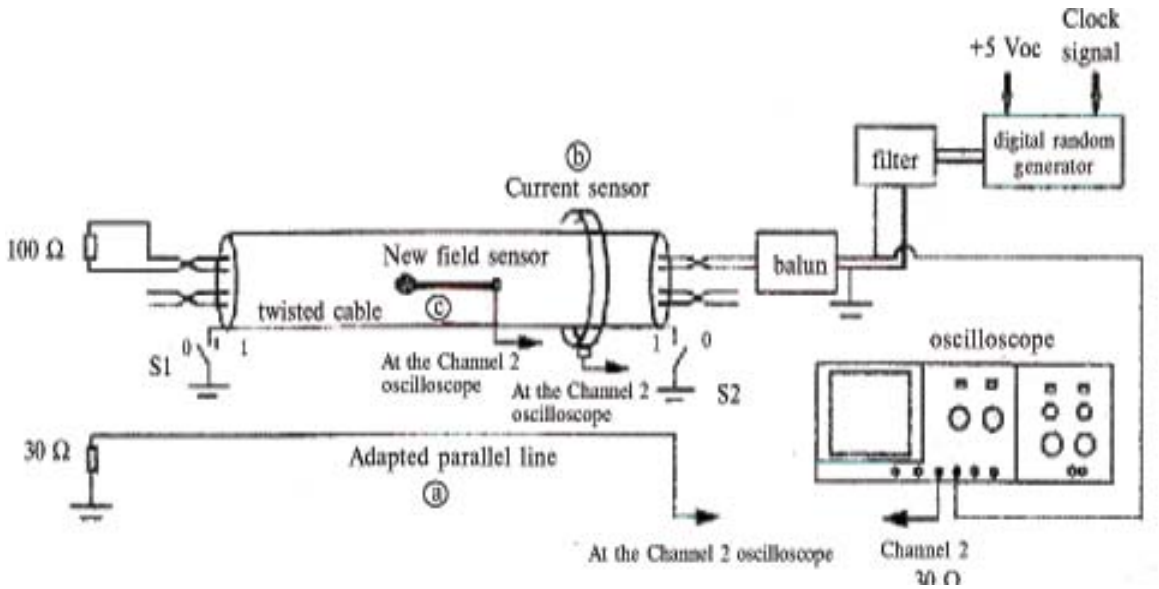

Рис. 1. *Схема измерительной установки (лаборатория Montena emc SA, Швейцария)*

Принятый сигнал после фильтрации подавался на вход осциллографа. После чего его сравнивали с исходным сигналом измеренным непосредственно в кабеле.

Результаты опытов, проведенных для нескольких наиболее распространенных сетей оказались неожиданными. Ожидалось, что переданный сигнал может быть восстановлен, но легкость, с которой это было сделано, удивительна. На рисунке 2 приведенны результаты измерения при «несимметричном режиме» передачи.

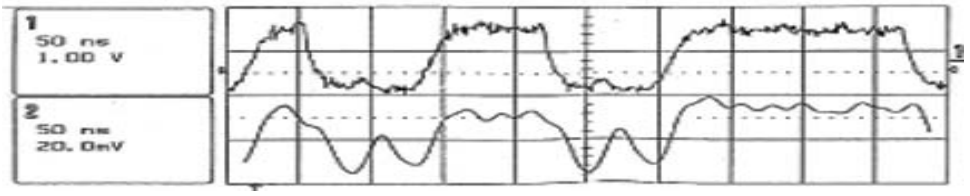

Рис. 2. *Исходный (вверху) и восстановленный (внизу) сигналы от кабельной линии.*

Результаты дальнейших исследований показали, что качество экранирования и соединения экрана кабеля с оборудованием сильно влияют на мощность излучения передаваемых данных. Также не менее важным является качество заземления активного и пассивного оборудования, поскольку даже очень хорошо экранированный кабель не обеспечивает безопасность передачи, если экран не соединен должным образом. Таким образом на ряду с качеством экранирования кабелей важным является правильное проведение монтажных работ, с учетом всех требований, иначе нельзя гарантировать

надежность линии. Однако все эти меры обеспечивают безопасность только от трех рассмотренных выше способов съема и обработки информации, при использовании более совершенных методов, безопасность не может быть гарантирована.

Выводы.

Безусловно, наиболее защищенными от несанкционированного съема информации через ПЭМИН канал являются волоконно-оптические сети. Для LAN, использующих медные кабеля, следует отдавать предпочтение экранированным системам. Так как согласно результатам исследования швейцарской компании Reichle & De-Massari AG неэкроанированные кабельные системы обеспечивают необходимый уровень безопасности только для низкоскоростных приложений. Кроме того чрезвычайно важным является качество монтажных работ, по соединению экранов и заземлению оборудования.

Список использованной литературы:

[1] Савчук Александр, *Проблемы технической защиты информации и электромагнитной совместимости для структурированных кабельных сетей.*
http://www.rdm.ua/download/TZI_Article.pdf
[2] Волобуев С.В., *Распространение сообщений по каналу ПЭМИ.*
http://ssl.stu.neva.ru/ssl/publications/magazine/1999/4/7/volobuev.pdf
[3] *Телефонные линии. Обнаружение и противодействие съему информации*.
http://das.kiev.ua/doc/teleph.doc
[4] Ананский Е.В., *Защита информации – основа безопасности бизнеса.*
http://www.bezpeka.com/library/secspec/ss_34.html
[5] Аркадий Вейц, *Защита информации от утечки по техническим каналам. ПЭМИН.*
http://www.pemin.ru/papers/paper1.html