разрушения ОПС и выбирая лучший. Для того чтобы избежать ухудшения надежности ОПС можно ограничить частоту, тогда равномерная последовательность ВЗ в условиях фильтрующей атаки должна измениться и стать коррелированной последовательностью с некоторой оптимизированной корреляционной функцией. Данные исследования будут изложены в последующей публикации.

Литература:

1. 1.Маракова И.И., Мараков Д.А. Методика оценки эффективности систем с цифровыми водяными знаками в рамках заданных ограничений / Захист інформації – 2002. - №2. – с.с.58-64.

Поступила 20.02.2003

УДК 681.3

С.А.Чеховский, Ю.М. Рудаков

Побочные излучения и защита информации в локальных сетях

В связи с бурным развитием локальных и глобальных вычислительных сетей широкое развитие получили и методы разведки (промышленного шпионажа), направленные на перехват информации, обрабатываемой (передаваемой, хранящейся) в локальных сетях. Причем, трудно уверенно сказать, кто сейчас больше занимается разведывательной деятельностью: государства против других государств или коммерческие фирмы против других фирм. Соответственно, бурное развитие получили и методы противодействия разведке. Как правило, проникновение в локальную сеть какой либо организации возможно только при недостаточно квалифицированной настройке всех элементов локальной сети (включая и каждую рабочую станцию) администратором системы. В случае же грамотной настройки, применения дополнительных программных и аппаратных средств, выполнении необходимых организационных мероприятий, шпионам необходимо изыскивать методы добывания информации, не связанные с необходимостью проникновения в локальную сеть. В связи с этим в последнее время «второе дыхание» получают методы перехвата информации по каналам побочных излучений и наводок (ПЭМИН) элементов локальной сети.

Методика защиты отдельных компьютеров достаточно хорошо проработана, подкреплена необходимыми нормативными документами. Задача же защиты информации от утечки по каналам ПЭМИН в локальной сети существенно сложнее, чем для автономно используемых устройств.

Защита активного оборудования и рабочих станций.

Источниками электромагнитных излучений в локальной сети являются, безусловно, рабочие станции (компьютеры) и активное сетевое оборудование. Для защиты от утечки информации по каналам побочных излучений и наводок применяется экранирование этого оборудования.

Для снижения уровня излучений активного оборудования локальной сети это оборудование лучше всего размещать в экранированном шкафу. В частности, можно рекомендовать шкафы производства Schroff GmbH типа «HF». В конструкции этих шкафов приняты специальные меры по улучшению экранирующих свойств, такие, как, например, пружинящие контакты по всему периметру дверцы (рис. 1).

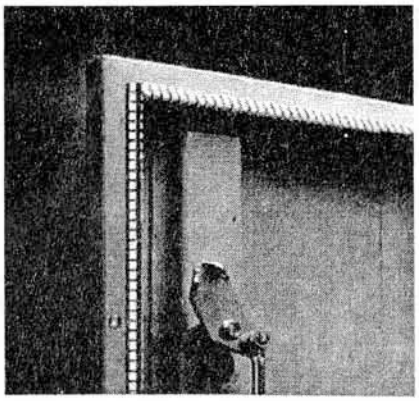

Рис. 1

Благодаря этому достигнуто ослабление радиочастотных сигналов свыше 80 дБ на частоте 30 МГц. На более высоких частотах уровень ослабления лежит в пределах от 40 до 70 дБ.

Хорошей практикой является размещение в этих же шкафах и серверов. Иногда в таких шкафах можно разместить и компьютеры. Однако чаще компьютеры устанавливаются на рабочих местах и, соответственно, приходится полагаться на экранирующие свойства их корпусов.

В настоящее время в Украине на рынке оборудования для средств вычислительной техники доступны корпуса очень высокого качества, в том числе и предназначенные для изготовления компьютеров, удовлетворяющих требования Европейской Директивы по электромагнитной совместимости (European EMS Directive 89/336/EEC). Однако, на уровень излучения существенно влияет качество всех элементов, устанавливаемых в компьютер, а не только качество его корпуса. Более того, требования по электромагнитной совместимости намного менее жесткие, чем требования по технической защите информации. ЕПОС совместно с НИИЭМП проводили исследование уровней излучения, создаваемых компьютерами в различных серийно выпускаемых корпусах. Результаты исследований показали, что современные корпуса позволяют значительно ослабить излучения элементов компьютера. Однако, за редким исключением, без дополнительной доработки ни один серийный корпус не может использоваться в качестве корпуса компьютера с защитой информации. Более того, качество экранирования корпуса системного блока компьютера влияет на уровень излучения всех устройств, подключенных к системному блоку (например, клавиатуры).

Стандартная клавиатура обычно имеет очень высокий уровень излучения. В тоже время с клавиатуры вводятся очень критичные с точки зрения безопасности данные, включая пароли пользователей и администратора системы. Излучение клавиатуры относительно узкополосное и сосредоточено, в основном, в области коротких и ультракоротких волн. Для его перехвата может использоваться очень дешевый коротковолновый разведывательный приемник. Учитывая также, что данные, вводимые с клавиатуры, вводятся в последовательном коде и поэтому могут быть легко интерпретированы, излучения, создаваемые клавиатурой, следует считать наиболее опасными.

Результаты же измерений уровня электрической (рис.2) и магнитной (рис.3) составляющих, проводимых ЕПОС совместно с НИИЭМП, показал, что у компьютеров с различными серийно выпускаемыми корпусами системных блоков мощность побочных излучений от клавиатуры может отличаться более чем в 100 раз.

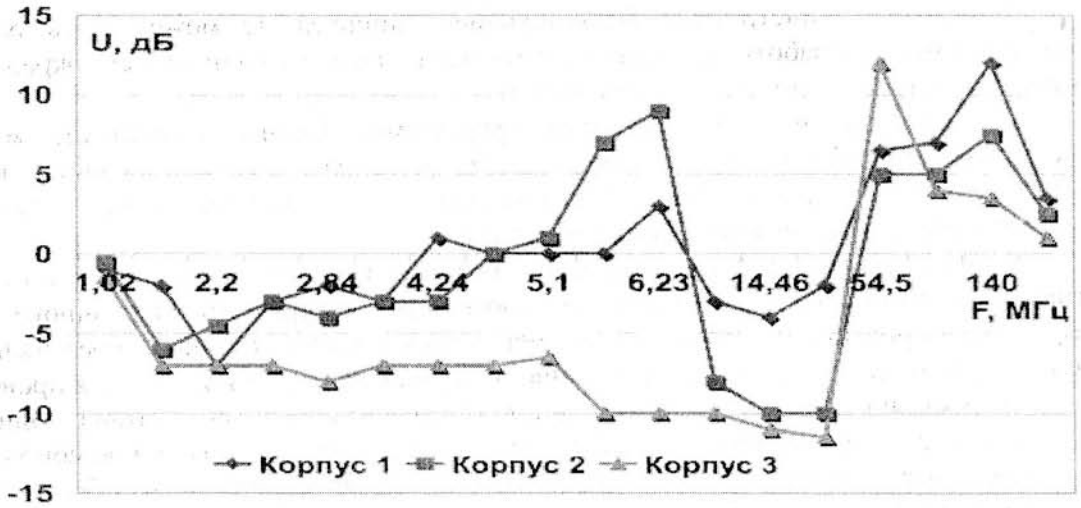

Рис. 2. Уровни электрической составляющей

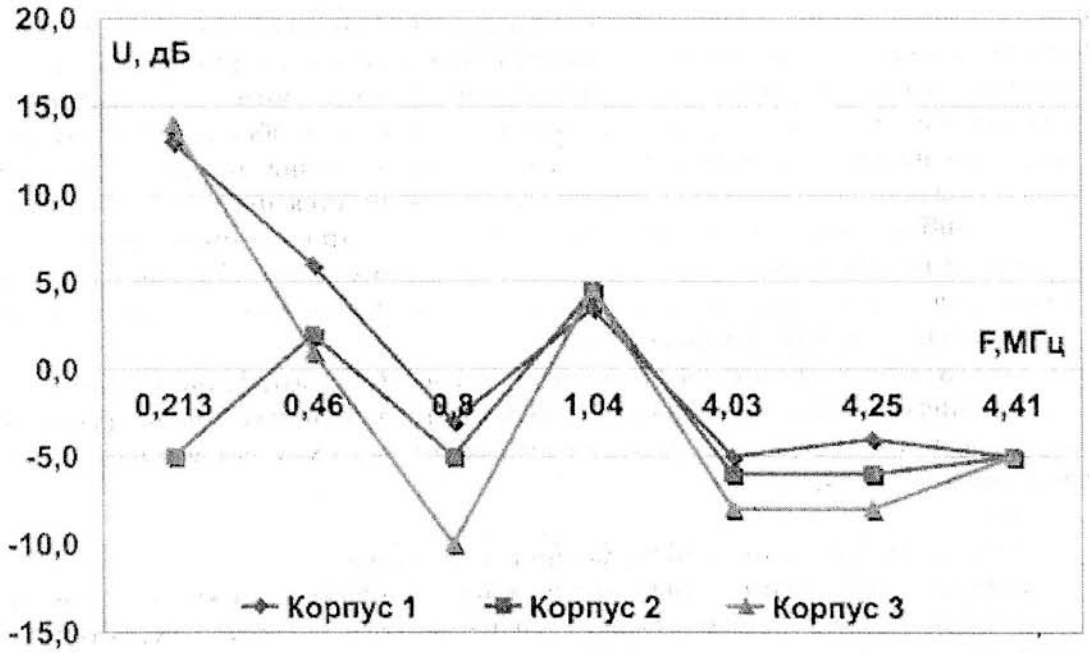

Рис. 3. Уровни магнитной составляющей

Аналогичные соотношения получаются и для других устройств, входящих в состав ПК.

Самый главный же вывод из результатов измерений неутешителен: при более или менее жестких требованиях по безопасности любой серийный корпус необходимо дорабатывать.

Задача доработки стандартных корпусов и шкафов, пусть даже с улучшенными характеристиками по электромагнитной совместимости, на первый взгляд простая, но в практической реализации оказывается далеко не тривиальной.

Во-первых, корпуса изготавливаются не из цельного куска металла. В местах соединения отдельных конструкций корпуса всегда есть щели, которых достаточно для того, чтобы существенно ухудшить экранирующие свойства.

Во-вторых, корпус электронного прибора, как правило, не может быть герметичным. Нужны вентиляционные отверстия для отвода тепла.

В третьих, конструкция экранирующего корпуса не может быть рассчитана заранее. Поэтому доработка стандартного корпуса с целью улучшения его экранирующих свойств это всегда экспериментальная работа.

Тем не менее, эти трудности разрешимы. Сейчас существует множество материалов, предназначенных для улучшения экранирующих свойств корпусов. (Всевозможные пружинящие уплотнители, электропроводящие эластомеры, самоклеющиеся металлизированные покрытия).

Еще больше хлопот приносит блок питания. Точнее говоря, не сам по себе блок питания, а необходимость подачи электроэнергии внутрь экранированного корпуса. Внутрь экранированного объема любой провод может заходить только через специальный фильтр, препятствующий распространению побочных излучений вдоль этих проводов.

В настоящее время теория фильтров очень хорошо проработана. Однако, для правильного расчета характеристик фильтра необходимо знать выходное сопротивление источника высокочастотных колебаний (блока питания активного оборудования) и входное сопротивление приемника этих колебаний (электрической сети, от которой данное оборудование запитывается). В нашем случае выходное сопротивление конкретного блока питания еще можно каким либо образом измерить. Но комплексное внутреннее сопротивление электрической сети мы не будем знать никогда. А оно в зависимости от протяженности линий электропитания, количества и характеристик подключенной к этой сети приборов может не только изменяться по величине, но и менять свой характер. На некоторых частотах комплексное сопротивление может носить емкостной характер, на некоторых индуктивный. И это сопротивление может изменяться при подключении к линии электропитания различных приборов. Поэтому разработка фильтра для подавления излучений в цепях электропитания это тоже большей частью экспериментальная работа. Хороший результат достигается путем большого количества проб и ошибок. Более того, ни один серийно изготавливаемый фильтр не может полностью выполнять свои функции в широкой полосе частот. Хорошие фильтры – это компромиссное решение, которое только в большинстве случаев удовлетворяет предъявляемым к фильтру требованиям.

Тем не менее, техника, в частности компьютеры, изготавливаются в защищенном от утечки информации по каналам ПЭМИН исполнении уже очень давно. И только конструкторы такой техники представляют, каким трудом удается получить требуемые характеристики.

Компьютеры с защитой информации и заземление.

Компьютеры с защитой информации могут использоваться как в составе локальной вычислительной сети, так и автономно. В зависимости от этого характеристики по защите информации от утечки по каналам ПЭМИН могут существенно отличаться. И основным фактором, приводящим к различию характеристик, является заземление устройств. Особенности заземления устройств в составе локальной сети мы рассмотрим несколько позже, после анализа побочных излучений кабельной системы.

Что же касается автономных устройств, то вопреки распространенному мнению заземление не улучшает и не ухудшает их экранирующих свойств.

Заземление необходимо только по требованиям техники электробезопасности.

Впрочем, учитывая сказанное выше, понятно, что из-за неидеальности экранирования определенное влияние заземление все же оказывает. Как правило, уровень побочных излучений при грамотно выполненном заземлении несколько снижается. Однако в некоторых случаях при подключении заземления уровень побочных излучений может и увеличиться. Поэтому нельзя однозначно утверждать, что заземление необходимо с точки зрения защиты информации от утечки по каналу ПЭМИН. И более того, чем качественнее выполнено экранирование корпуса (включая и качество фильтров

в цепях электропитания), тем меньше сказывается на уровне побочных излучений наличие или отсутствие заземления.

Побочные излучения кабельной системы

Кабельная система не содержит активных или нелинейных элементов, поэтому сама по себе она не может быть источником побочных излучений. Однако кабельная система связывает между собой все элементы компьютерной сети. По ней передаются сетевые данные, но вместе с этим она является также приемником всех наводок и средой для переноса побочных электромагнитных излучений (рис.4).

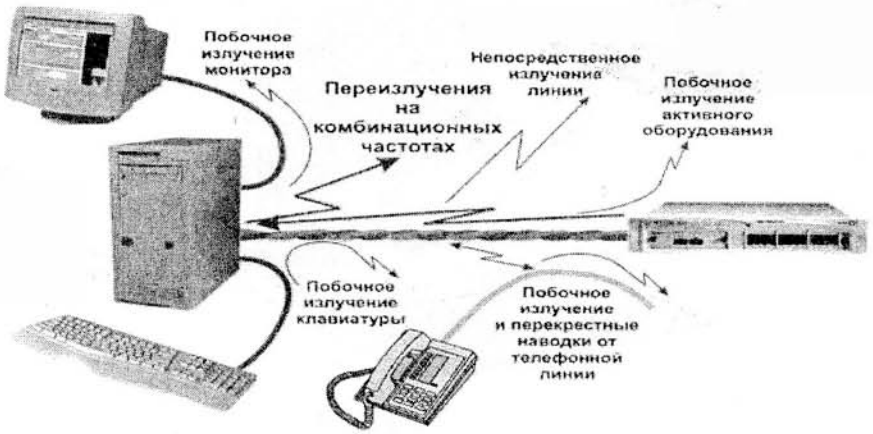

Рис. 4

Поэтому следует различать:

- Побочное излучение, вызванное передаваемыми по данной линии сигналами (трафиком локальной сети);
- прием и последующее переизлучение побочных излучений от расположенных вблизи других линий и устройств;
- излучение кабельной системой побочных колебаний от элементов сетевого активного оборудования и компьютеров, к которым подключен кабель.

Довольно часто при оценке защищенности кабельной системы интересуются только тем, насколько ослабляется побочное излучение, вызванное сигналами, передаваемые по кабелю в процессе сетевого обмена информацией. Все понимают, что если по радиоизлучению кабельной системы можно восстановить трафик в локальной сети, то это представляет большую опасность. На самом деле трафик локальной сети достаточно хорошо защищен от утечки информации по каналам ПЭМИН и без нашего участия. Современные кабели для локальных сетей имеют очень низкий уровень излучения передаваемых сигналов. В этих кабелях сигналы передаются по витой паре проводов, причем количество скруток на единицу длины строго постоянно. Благодаря этому витая пара получается очень хорошо сбалансированной. В принципе такая система вообще не должна излучать. Более того, наличие экрана у витой пары очень мало влияет на уровень излучения сигналов, передаваемых по витой паре.

Правда, в реальной системе всегда имеют место отдельные неоднородности кабеля. В первую очередь они возникают при небрежной или неквалифицированной прокладке кабеля. На местах поворотов кабеля в случае резкого изгиба изменяется взаимное положение проводников в витой паре и, как следствие, изменяется волновое сопротивление. Кроме того, большое влияние оказывает качество заделки кабеля в коннекторы. Более того, количество скруток на единицу длины в разных парах одного кабеля разное, к тому же каждый производитель имеет свое мнение по вопросу, сколько скруток на единице длины должно быть. Да и конструкция коннекторов у разных производителей разная. Все это, безусловно, влияет на уровень побочного излучения, возникающего в процессе сетевого обмена. Тем не менее, уровень излучения сигналов,

передаваемых по кабелю, остается довольно низким, особенно для кабелей категории выше пятой. Реально на расстоянии буквально единиц метров уже невозможно по электромагнитному излучению современного кабеля перехватить передаваемую по нему информацию.

Но в большинстве практических случаев кабельная система - это отличная антенна для всех побочных излучений оборудования, подключенного к сети. Побочные излучения, возникающие в элементах компьютера, наводятся на все провода кабеля локальной сети (рис.5).

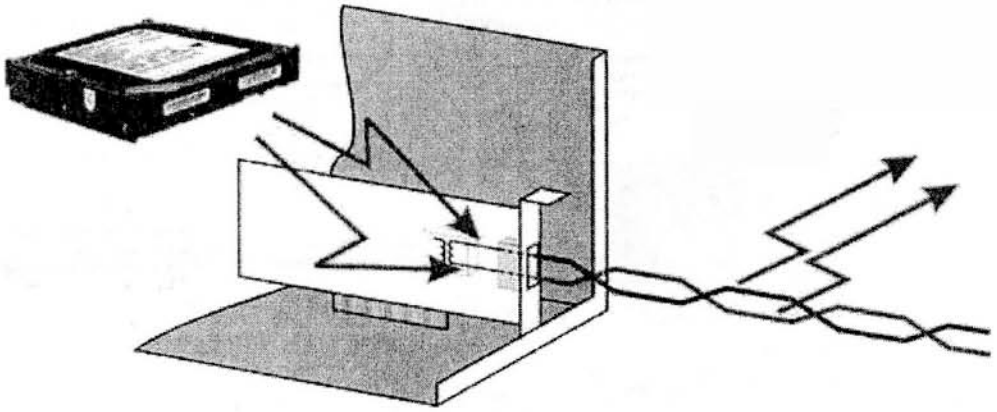

Рис. 5

Вследствие этого для побочных излучений элементов компьютера кабель локальной сети нельзя рассматривать как витую пару. Его необходимо рассматривать просто как одиночный многожильный провод, выходящий за пределы экранированного объема. Поставить для этих проводов фильтр, подавляющий побочные излучения, невозможно. Ведь побочные излучения элементов компьютера (жесткий диск, клавиатура и т.п.) сосредоточены в той же полосе частот, что и спектр импульсов, передаваемых по витой паре в процессе сетевого обмена. Подавляя побочные излучения, мы подавим и сетевой трафик. Таким образом, если компьютер с защитой информации включить в локальную сеть на неэкранированной витой паре, то провода неэкранированной витой пары, играя роль антенны, могут усилить напряженность поля, создаваемого, например, клавиатурой компьютера (см. рис.2, рис.3), в десятки тысяч раз. Поэтому неэкранированная витая пара не может применяться в локальной сети, в которой обрабатывается информация с ограниченным доступом.

Применение же экранированной витой пары значительно улучшают ситуацию, но не гарантирует подавления синфазных наводок. Причин для этого в локальной сети,много, но основная – заземление устройств, входящих в состав локальной сети.

Заземление в локальной сети

По технике электробезопасности все активное оборудование, входящее в состав локальной сети, должно иметь защитное заземление. Защитное заземление активного оборудования слабо влияет на излучение информации, циркулирующей в локальной сети. Но оно коренным образом изменяет способность кабелей локальной сети излучать синфазно наведенные на эти кабели колебания, вызванные работой элементов компьютера. Рассмотрим эквивалентную схему участка локальной сети для побочных излучений элементов компьютера (рис.6):

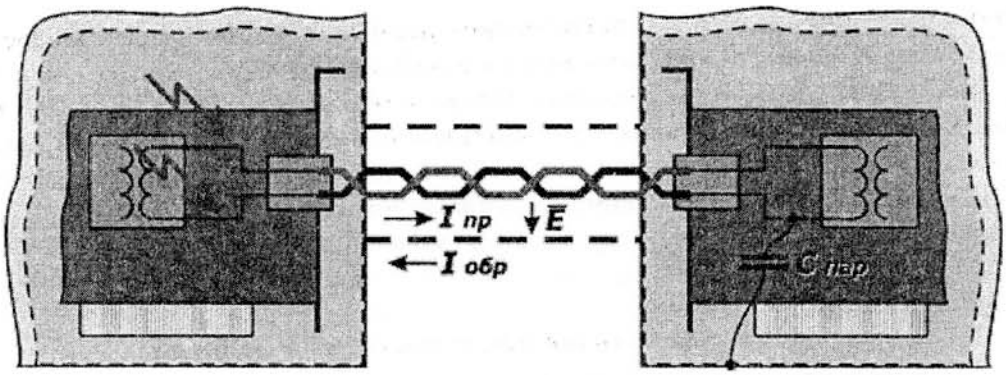

Рис. 6

Побочные излучения элементов компьютера наводятся синфазно на провода кабельной системы. Электрическое поле E, создаваемое наведенным излучением, локализуется в пространстве между жилами кабеля и экранирующей оплеткой. Поэтому оно очень хорошо подавляется (по крайней мере, при применении высококачественных кабелей). Наведенное напряжение приводит к появлению наведенного тока по жилам кабеля Iпр. и его оплетке Iобр. В отсутствии заземления магнитное поле, вызванное протеканием наведенного тока по жилам кабеля, компенсируется магнитным полем, вызванным протеканием этого тока во встречном направлении по оплетке кабеля. Поэтому в незаземленной системе побочные излучения элементов компьютера, проникающие в экранированные кабели локальной сети, может быть хорошо подавлено.

В том случае, если все активное оборудование заземлено, излучение элементов компьютера также вызывает появление наведенного тока Iпр. по жилам кабеля. Однако обратный ток в этом случае протекает как по экранирующей оплетке кабеля Iобр., так и по проводам заземления I'обр. (рис.7).

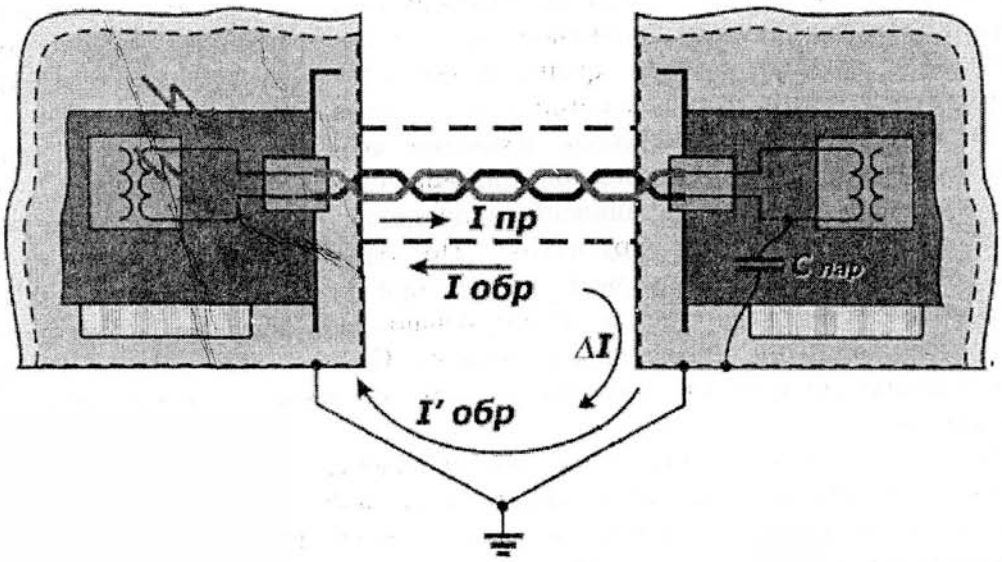

Рис. 7

В результате в контуре, образованном экранирующей оплеткой кабеля и проводами (шинами) заземления образуется разностный ток ΔI. Поэтому рассматриваемый контур для наведенного тока в кабеле, оплетке и цепях заземления представляет собой рамочную антенну, иногда просто гигантских размеров. Именно этот эффект и приводит к тому, что при подключении хорошо защищенного компьютера к локальной сети уровень излучений компьютера (в первую очередь, магнитной составляющей) значительно возрастает независимо от того, экранированные кабели применяются или нет. Особенно хорошо данный эффект проявляется на относительно низких частотах. А ведь во многих случаях

именно подавление магнитной составляющей на низких частотах представляет трудности даже для автономного (не подключенного к локальной сети) устройства (см. рис.3).

Важно отметить, что рамочная антенна образуется независимо от того, каким образом и как качественно выполнено заземление. Устранить это явление рациональным выбором системы заземления нельзя. Единственный способ уменьшить излучение – это подключение защитного заземления к каждому элементу локальной сети через фильтр, который обладает большим сопротивлением в широкой полосе частот, но малым сопротивлением на частоте 50 Гц.

Сеть локальная как часть сети глобальной

Локальная компьютерная сеть в настоящее время уже не может эксплуатироваться автономно, без взаимодействия с другими сетями. В частности, любая организация, будь то частное предприятие или орган государственного управления, должна быть активно представлена в глобальной сети интернет. Это и собственный сайт, и общедоступная электронная почта, и доступ сотрудников к информации глобальной сети. Такое тесное взаимодействие вступает в конфликт с требованиями обеспечения безопасности.

При взаимодействии нескольких сетей могут возникать различные угрозы безопасности. Например, при подключении к глобальной сети интернет самой безобидной из возможных угроз является взлом сети из хулиганских побуждений. Наиболее типичное проявление вандализма в интернет – замена существующих ссылок на ссылки порнографических сайтов. Это, по крайней мере, вредит имиджу владельца сайта и приводит к дополнительным материальным затратам на восстановление всех ссылок.

В компьютерных сетях государственных органов власти циркулирует информация, представляющая интерес для иностранных разведок. Эта информация может не иметь грифа секретности. Однако в совокупности позволяет получить довольно важные сведения. Поэтому, в случае объединения компьютерных сетей государственных органов с глобальной сетью интернет кроме хулиганских взломов следует предполагать и более квалифицированные попытки проникновения в сеть сотрудников иностранных разведок. Противостоять таким попыткам крайне сложно. Поэтому сеть интернет необходимо изолировать от внутренней сети, в которой сосредоточены обобщенные данные.

Известно несколько способов изоляции собственной компьютерной сети от глобальной сети интернет с целью обеспечения безопасности. В сетях, в которых не циркулирует информация с ограниченным доступом, для изоляции сетей как правило достаточно использовать маршрутизатор. Но серьезную защиту от вторжения из глобальной сети можно обеспечить только при применением межсетевых экранов (FireWall). Поэтому для защиты корпоративной информации коммерческих фирм необходимо применение межсетевых экранов. Однако, для защиты информации в государственных органах как правило межсетевой экран не обеспечивает требуемого уровня защиты.

Наиболее полно безопасность обеспечивается только в случае физической изоляции сети интернет от собственной локальной сети. Безусловно, это создает определенные неудобства в работе и требует дополнительных затрат при создании компьютерной сети. Однако в условиях необходимости противодействия иностранным разведкам это оправданная мера. Именно поэтому в Украине постановлением Кабинета Министров от 12.04.2002 года запрещено подключать к глобальным сетям вычислительные сети и отдельные компьютеры, на которых обрабатывается или хранится информация с ограниченным доступом, собственником которой является государство.

При построении сетей с физической изоляцией также необходимо учитывать вопросы защиты от утечки информации по каналам ПЭМИН. Во многих случаях сотруднику, работающему с информацией ограниченного доступа необходима и возможность выхода в интернет. Решается этот вопрос, как правило «в лоб». На рабочем месте устанавливается два компьютера, один из которых подключен к локальной сети

предприятия (организации), а второй к сети интернет. В этом случае кабели собственной сети с защитой информации и кабели открытой сети интернет очень трудно разнести на достаточное расстояние. Вследствие этого информация, циркулирующая в локальной сети, а также все побочные излучения компьютеров, наведенные на кабели локальной сети, могут наводиться и на кабели открытой сети интернет. Мало того, что кабель открытой сети это достаточно длинная антенна (особенно когда открытая сеть проложена неэкранированным кабелем). Кабели открытой сети как правило выходят за границы охраняемой территории, поэтому снять информацию можно не только путем перехвата излучений, но и путем непосредственного подключения к кабелям открытой сети. Поэтому кабели открытой сети также должны быть проложены в соответствии со всеми рекомендациями, выполняемыми при построении сети с защитой информации.

Поступила 27.02.2003

УДК 681.3

Головань С.М., Давиденко А.М., Щербина В.П.

ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ КОНТРОЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ ТА ПЕРЕПУСКНОГО РЕЖИМУ

Одним із важливих заходів забезпечення захисту інформації з обмеженим доступом на підприємствах, в установах і організаціях є регулярний контроль. Але останнім часом відбувається значне збільшення обсягів контрольної інформації, що веде до збільшення витрат. Спробуємо розглянути цю проблему з точки зору необхідності, періодичності та якості контролю.

Контроль – перевірка, облік діяльності кого-, чого-небудь, нагляд за кимось, чимось [2].

Контроль здійснюється з метою оцінки дотримання законодавчих актів України, фактичного стану захисту інформації з обмеженим доступом, виявлення недоліків і порушень, встановлення їх причин, вироблення заходів спрямованих на усунення та попередження цих недоліків і порушень.

Контроль повинен мати системний характер і, як правило, він складається з двох частин. Перша – постійно здійснюється оперативний контроль за станом роботи підрозділу з захисту інформації з обмеженим доступом. Друга – періодично організується відповідно до заздалегідь складеного графіку перевірки за станом забезпеченням захисту інформації з обмеженим доступом.

Контроль поділяються на:

– комплексний, при проведенні якого всебічно перевіряється організація та стан захисту інформації з обмеженим доступом;

– цільовий, при проведенні якого перевіряються окремі питання діяльності та виконання вимог розпорядчих документів;

– перевірочний, коли перевіряється виконання пропозицій щодо виправлення помилок та усунення недоробок (за актами, довідками перевірки тощо).

Перевіряючий знайомиться з усіма документами, які мають відношення до питання, що перевіряється, а також проводить бесіди і консультації з фахівцями і виконавцями, при цьому необхідно використати такий обсяг матеріалу, який дозволив би зробити підсумок стану роботи в напрямку діяльності, що вивчався.

Задачі контролю: