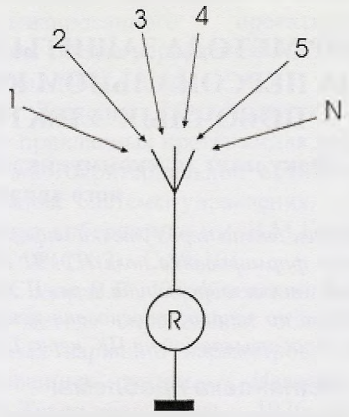
па

ми



K=R/(R

от

ники

мето-

При энергетической маскировке излучается широкополосный шумовой сигнал с уровнем, существенно превышающим во всем частотном диапазоне уровень излучений ПК. Одновременно происходит наводка шумовых колебаний в отходящие цепи. Возможности энергетической активной маскировки могут быть реализованы только в случае, если уровень излучений ПК существенно меньше норм на допускаемые радиопомехи от средств ВТ. В противном случае устройство активной энергетической маскировки будет создавать помехи различным радиоустройствам, расположенным поблизости от защищаемого средства ВТ, и потребуется согласование его установки со службой радиоконтроля. Из устройств активной энергетической маскировки наиболее известны: «Гном», «Шатер», «ИнейТ», «Гамма».

Неэнергетический метод активной маскировки заключается в изменении вероятностной структуры сигнала, принимаемого приемником злоумышленников, путем излучения специального маскирующего сигнала. Исходной предпосылкой в данном методе является случайный характер электромагнитных излучений ПК.

Активный метод хорош тем, что устраняется не только угроза утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы. Как правило, становится невозможным также и применение закладных подслушивающих устройств. Становится невозможной разведка с использованием излучения всех других устройств, расположенных в защищаемом помещении.

Недостатки: достаточно мощный источник излучения является опасным для здоровья, а наличие маскирующего излучения свидетельствует, что в данном помещении есть серьёзные секреты, что будет привлекать повышенный интерес недоброжелателей. После установки источников шума необходимо проведение сложных измерений по всему периметру охраняемой зоны и для всех частот. Процедуру проверки необходимо повторять всякий раз, когда просто меняется расположение компьютеров, не говоря уж об установке новых. В следствие, техническое обслуживание таких систем зашумления может быть слишком дорогим.

Пассивный метод. Пассивный метод заключается в экранировании источника излучения (доработка компьютера), размещении источника излучения (компьютера) в экранированном шкафу или в экранировании помещения целиком. Экранирование ПК – это весьма сложный процесс. Поэтому цена экранированного ПК достаточно высока.

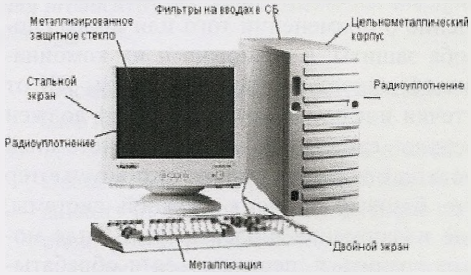


Рис.3. Технология защиты ПК от ПЭМИ

Современные технологии основаны на нанесении (например, напылении) различных специальных материалов на внутреннюю поверхность существующего корпуса, поэтому внешний вид компьютера практически не изменяется. Только при очень внимательном рассмотрении можно заметить несколько увеличенные зазоры в отдельных элементах. Да ещё заменены шнуры и некоторые разъёмы. Доработка уже имеющегося компьютера обойдется руководителю на 20-30 % дороже готового защищенного ПК.

Некоторыми строительными нормами предусматривается экранировка помещений, в которых расположена вычислительная техника. Так, например, ведомственными нормами ВБН В.2.2-00032106-1-95 для банковских учреждений предусматривается экранирование серверной и некоторых других помещений. Регламентирована и эффективность экранирования. Однако, когда осуществляется сплошное экранирование с помощью ме-

таллического листа, эффективность экранирования может получиться неудовлетворительной. Выполнение экранировки требует значительных экономических затрат, регулярного контроля эффективности и большого расхода материалов, весьма трудоемко, сложно в изготовлении входов в помещения вентиляции и вводов коммуникаций.

Выводы

Универсального, на все случаи жизни, способа защиты информации от перехвата через ПЭМИ ПК, конечно же, не существует. В каждом конкретном случае специалистами должно приниматься решение о применении того или иного способа защиты, а возможно и их комбинации. В основе построения защиты ПК от утечки информации через ПЭМИ должен лежать системный подход. Системный подход показывает также, что компьютер это базовый элемент сложной системы, где информация в электронном виде может храниться, передаваться и обрабатываться. При этом каждому состоянию информации соответствует определенная конфигурация вычислительных средств и должны соответствовать определенные меры защиты этой информации. И все же для большинства малых средних фирм оптимальным способом защиты информации с точки зрения цены, эффективности защиты и простоты реализации представляется приобретение компьютеров в уже защищенном виде. В целом, конечно, для защиты информации пригодны оба метода. Но при одном условии: если у фирмы есть подтверждение того, что принятые меры действительно обеспечивают требуемую эффективность защиты.

Список литературы

1. Домарев В.В. Безопасность информационных технологий. Системный подход. - К.: ООО ТИД «Диасофт», 2004.- 992с.

2. Домарев Д. Побочные электромагнитные излучения персонального компьютера и защита информации, 2006. http://security.to.kg/comp/pemin.htm

3. Аркадий Вейц. Защита информации от утечки по техническим каналам. ПЭМИН
http://www.pemin.ru/papers/paper1.html

4. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие для подгот. экспертов системы Гостехкомиссии России. — М.: Горячая линия-Телеком, 2005. — 414с.

5. Сорокин А.Д. Побочные электромагнитные излучения (ПЭМИ) компьютера. http://www.electrosad.narod.ru/

6. ТР ТЗІ - ПЕМВН-95. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. – Введ. 01.07.95. К.: ДСТЗІ СБ України, 1995.