

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://studservis.ru/gotovye-raboty/referat/294397>

Тип работы: Реферат

Предмет: Информатика

Утечка информации за счет электромагнитных излучений и наводок

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА I. ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ.....	5
1.1 Определение предельного значения опасного сигнала, наводимого ПЭВМ	9
ГЛАВА II. ПОНЯТИЕ И СУЩНОСТЬ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК.....	13
2.1 Общая характеристика технических каналов утечки информации.....	15
ЗАКЛЮЧЕНИЕ.....	20
СПИСОК ЛИТЕРАТУРЫ.....	21

ВВЕДЕНИЕ

Под информацией обычно понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа) . Информация ограниченного доступа – информация, содержащая сведения, отнесенные к государственной тайне, а также сведения конфиденциального характера (персональные данные, сведения, составляющие коммерческую, служебную и иную тайну, и т.д.).

Это, как правило, защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации .

ГЛАВА I. ЭЛЕКТРОМАГНИТНЫЕ ИЗЛУЧЕНИЯ ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРОВ

Проблема утечки данных через электромагнитное излучение и помехи (ПЭМИН) известна специалистам уже более 20 лет. И только в последние годы это стало обсуждаться на страницах открытой литературы. В основном это связано с самым широким распространением персональных компьютеров (ПК). Практически любая организация, будь то коммерческое предприятие или государственное предприятие, сегодня не может существовать без использования вычислительной техники. Работа персонального компьютера, как и любого другого электронного устройства, сопровождается электромагнитным излучением в диапазоне радиочастот. Для ПК эти излучения регистрируются в диапазоне частот до 1 ГГц, максимум в диапазоне от 50 МГц до 300 МГц. Такой широкий спектр излучения объясняется тем, что в ВТ-устройствах информацию несут последовательности прямоугольных импульсов короткой продолжительности. Следовательно, непреднамеренное излучение содержит компоненты, частоты которых являются как первыми гармониками, так и гармониками более высокого порядка. Появление дополнительных компонентов в побочном электромагнитном излучении также приводит к использованию высокочастотной коммутации в ВТ. Нет необходимости говорить о какой-либо диаграмме направленности электромагнитного излучения компьютера, поскольку на практике расположение его компонентов (системного блока, монитора, соединительных кабелей и силовых проводов) относительно друг друга представляет собой неограниченное количество комбинаций. Поляризация излучения ПК линейна. В конечном итоге это определяется расположением соединительных кабелей, поскольку они являются основными источниками излучения в компьютерах, в которых системный блок имеет металлическое покрытие. Помимо излучаемого электромагнитного поля вблизи работающего компьютера, существуют квазистатические магнитные и электрические поля, которые быстро уменьшаются с расстоянием, но вызывают помехи для любых

проводящих цепей (металлических труб, телефонных проводов, проводов системы пожарной безопасности и т. д.). Эти поля важны на частотах от десятков килогерц до десятков мегагерц. Очевидно, что этого уровня радиации достаточно для перехвата на значительных расстояниях. Таким образом, соответствие электромагнитного излучения средств ВТ нормам электромагнитной совместимости не гарантирует сохранения конфиденциальности обрабатываемой в них информации. Кроме того, следует отметить, что значительная часть российского парка ПК даже не соответствует этим стандартам, так как в погоне за дешевизной в страну ввозились в основном устройства "желтой" сборки, не имевшие сертификатов качества.

1.1 Определение предельного значения опасного сигнала, наводимого ПЭВМ

Утечка информационного сигнала через электрические цепи может происходить несколькими способами. Например, между двумя электрическими цепями, расположенными на определенном расстоянии друг от друга, могут возникать электромагнитные связи, которые создают объективные предпосылки для появления информационного сигнала в цепях энергосистемы компьютерного оборудования (ВТ), которые не предназначены для передачи этого сигнала и могут образовывать неконтролируемые каналы утечки информации. Эти процессы называются наводками и подразумевают передачу энергии от одного устройства к другому, что не предусмотрено схемой или конструктивными решениями.

В литературе наводки рассматриваются как набор из трех элементов: источника, приёмника и паразитной связи между ними. В связи с рассматриваемой проблемой источниками помех являются устройства, в которых обрабатывается информационный сигнал; приемники- силовые цепи, выступающие в качестве проводящей среды, выходящей за пределы контролируемой территории и в то же время представляющие собой опасный канал утечки информации, обрабатываемой ПЭВМ и ЛВС.

Основная опасность паразитных наводок заключается в возможности создания одновременно нескольких источников информационного сигнала и через множество паразитных коммуникационных цепей. В большинстве радиоэлектронных систем и ВТ-устройств вторичный источник питания (ВИП) и система распределения питания являются общими для многих элементов, блоков и узлов, в соответствии с идеальными требованиями цель системы распределения питания состоит в том, чтобы обеспечить максимально стабильное напряжение для всех нагрузок (цепей и устройств) в условиях изменения потребляемых ими токов. Кроме того, любой сигнал переменного тока, генерируемый нагрузкой, не должен создавать переменное напряжение на линиях питания.

ЗАКЛЮЧЕНИЕ

Несмотря на то, что для большинства руководителей предпринимательских структур утечка конфиденциальной информации из используемой ВТ через ПЭМИН кажется маловероятной, такой канал перехвата информации все же существует, а это значит, что рано или поздно кто-то им все-таки воспользуется. Особую остроту эта проблема приобретает для коммерческих фирм, офисы которых занимают одну или несколько комнат в здании, где кроме них размещаются другие организации.

1. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
2. Взамен: ГОСТ Р 51275-99; введ. 2008-02-01. - М.: Стандартинформ, 2014. - 6 с.
3. Доктрина информационной безопасности Российской Федерации (Принята 9 сентября 2000 г. № ПР-1895).
4. Терминология в области защиты информации: Справочник. М.: ВНИИ Стандарт, 1993. -110 с.
5. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия РФ, 2012. 320 с.
6. ГОСТ Р 50922- 2006. Защита информации. Основные термины и определения. - Введ. 2008-02-01. - М.: Стандартинформ, 2007. - 12 с.
7. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ: [принят Гос. Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г.]. [Электронный ресурс]. - Режим доступа: <http://www.rg.ru/2006/07/29/informacia-dok.html>
8. Техническая защита информации. Основные термины и определения: рекомендации по стандартизации Р 50.1.056-2005: утв. Приказом Ростехрегулирования от 29 декабря 2005 г. № 479-ст . - Введ. 2006-06-01. - М.:

Стандартинформ, 2006. - 16 с.

9. ГОСТ 24375-80. Радиосвязь. Термины и определения. - Введ. 1982-01-01. - М.: Стандартинформ, 2005. - 123 с.

10. Хорев А.А. Техническая защита информации: учеб. пособие для студентов ву-зов. В 3 т. Т. 1. Технические каналы утечки информации. М.: НПЦ «Аналитика», 2008. - 436 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой:

<https://studservis.ru/gotovye-raboty/referat/294397>