Практическая работа №6:«Защита информации от утечки по электромагнитному каналу пассивными методами»

6.1 Краткие теоретические сведения

Побочные электромагнитные излучения и наводки (ПЭМИН) являются наиболее опасным техническим каналом утечки информации средств вычислительной техники (СВТ). Выполнение нормативов по ПЭМИН на объектах информатизации гарантирует конфиденциальность обрабатываемой СВТ информации. Обычно для выполнения указанных нормативов применяют активную радиотехническую маскировку побочных излучений, электромагнитную экранировку помещений, рабочих мест и объектов информатизации или самих СВТ. Это сопровождается рядом недостатков, в том числе существенным удорожанием защиты за счёт дооборудования генераторами помех объекта информатизации и необходимостью оценки санитарного состояния последнего, ярко выраженным отрицательным влиянием на организм пользователя.

Soft Tempest технология. В качестве управляемого канала передачи данных можно использовать ПЭМИН компьютера. Soft Tempest – технологии скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств.

Soft Tempest атака позволяет с помощью специальной программы-закладки, внедряемой с использованием стандартной техники применения «вирусов», «червей» и «троянцев», искать необходимую информацию в компьютере и передавать ее путем модуляции изображения монитора. Принимая побочные излучения монитора можно выделить полезный сигнал и таким образом получить информацию, хранящуюся в компьютере.

Простейший способ Soft Tempest атаки использует амплитудную модуляцию экранного изображения и стандартный АМ-приемник. При передаче информации этим простейшим способом на экране монитора возникает характерное изображение, вид которого определяется частотой амплитудной модуляции (рисунок 6.1).

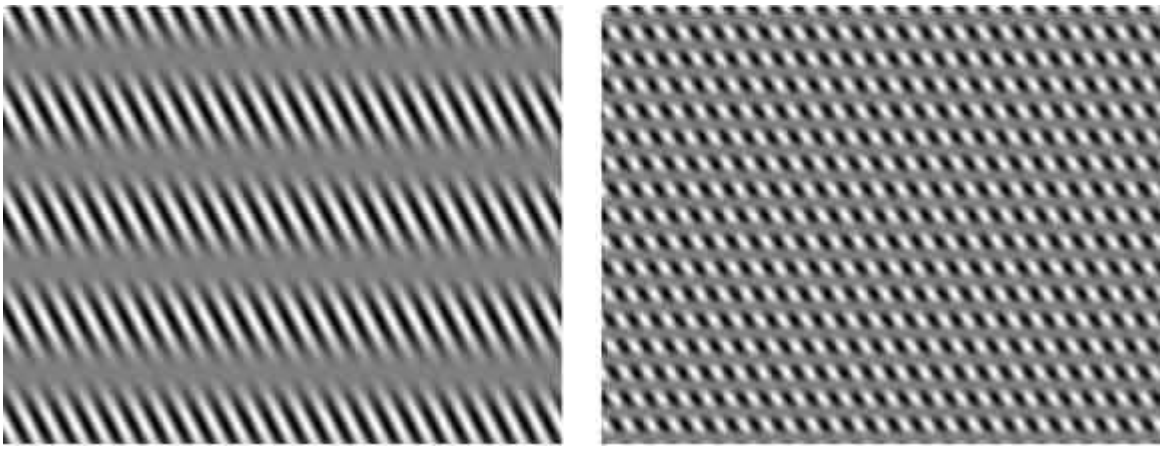

Рисунок 6.1 – Изображение на экране монитора при амплитудной модуляции тоном разной частоты

Подобную «рябь» на мониторе трудно не заметить. Таким образом, при передаче информации путем управления излучением монитора сталкиваются с необходимостью решения задачи стеганографии в классической постановке (совокупность средств и методов, используемые для формирования скрытого канала передачи информации).

Задача встраивания интересующей информации решается путем подбора характеристик управляющих сигналов, чтобы информация, излучаемая в эфир, отличалась от

отображаемой на экране монитора. Причем, это возможно не только для текстовой информации, но и для графической.

Утечка информации через порты ПК. Одним из самых лучших методов скрытой передачи информации – передача по каналу, который не охвачен контролем. В этом плане конечно лучше всего предавать информацию посредством электромагнитных излучений компьютера.

Обращение к любому устройству и даже к любому незадействованному порту вызывает появление побочных излучений на определенных, характерных для данного порта, частотах и с определенной мощностью. Поэтому Soft Tempest атаки могут существовать во множестве вариантов, в зависимости от того, какое конкретно устройство компьютера выбрано для управления излучением. При этом и программа – закладка может быть значительно проще, чем в рассмотренном выше случае, так как и вывод в порт программно реализуется проще, чем формирование специальных кодов для модуляции луча трубки монитора, и не требуется применения стеганографических методов. Скрытность передачи обеспечивается тем, что сегодня отсутствуют штатные средства контроля излучений компьютера. Использование обычных сканирующих приемников для целей контроля малоэффективно вследствие того, что компьютер излучает в широкой полосе частот, и отыскать в этой полосе частот ту, на которой осуществляется передача, очень сложно.

Интерес к последовательному порту вызван особенностью его конструктивного исполнения. Передача «1» и «0» осуществляется импульсами разной полярности с амплитудой более 5 В. Это позволяет предположить, что уровень излучений, вызванной передачей в порт информации, будет достаточно высоким, даже если к порту никакие устройства не подключены (соответственно, отсутствует более-менее эффективная антенна). Кроме того, последовательная передача легко перехватывается и интерпретируется. К тому же последовательный порт позволяет программно задавать скорость передачи.

Изменение скорости передачи данных в порт, можно получить на отдельных частотах существенное превышение уровня излучения порта над уровнем излучения остальных элементов компьютера. Если к порту подключено какое-либо устройство, то соединительный кабель играет роль антенны. В этом случае уровень излучения получается настолько высоким, что принимать информации можно весьма примитивными средствами на значительном расстоянии.

Но наиболее интересные результаты получаются при скорости передачи 9600. Результаты измерения уровней излучения для случая, когда к порту не подключены никакие устройства при скорости передачи 9600, приведены на рисунке 6.2.

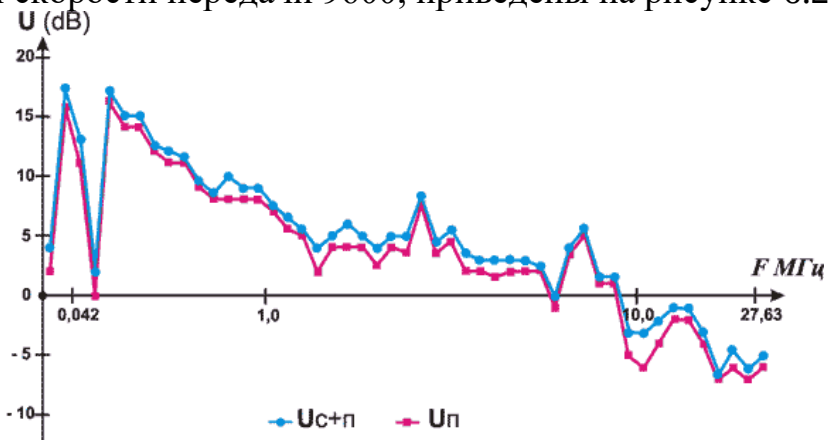

Рисунок 6.2 – Уровни излучения компьютера через последовательный порт

Красная линия, $U_п$, соответствует значениям уровня излучения компьютера при отсутствии передачи информации через излучение последовательного порта. Синяя линия, $U_{с+п}$, - уровням излучения в моменты передачи информации.

Анализ приведенного графика показывает, что абсолютное значение уровня побочных излучений при выводе информации в незадействованный последовательный порт на отдельных частотах может быть весьма значительным. Однако, превышение этого уровня над уровнем остальных побочных излучений компьютера во всем диапазоне частот остается небольшим. В лучшем случае отношение сигнал/шум составляет 2–3 дБ.

Такая величина говорит о том, что обнаружить работу программной закладки, передающей информацию через побочные излучения последовательного порта, практически невозможно.

Таблица 6.1 – Электромагнитное излучение компьютера

Источник излучения	Диапазон частот
сетевой трансформатор блока питания	50 Гц
преобразователь напряжения в импульсном блоке питания	20 – 100 кГц
кадровая развертка	40 – 160 Гц
строчная развертка	15 – 110 кГц
ускоряющее анодное напряжение монитора	0 Гц
системный блок	50 Гц – 4 ГГц
устройства ввода-вывода информации	0 – 50 Гц
источник бесперебойного питания	20 – 100 кГц

Естественно, не весь спектр электромагнитного излучения компьютера может быть использован для перехвата информации. Интерес в этом отношении представляют лишь цепи, по которым передается информация. Поэтому электрические цепи компьютера можно разделить на информативные и неинформативные. Для персонального компьютера информативными ПЭМИН являются излучения, формируемые следующими цепями:

– цепь, по которой передаются сигналы от контроллера клавиатуры к порту ввода-вывода на материнской плате;

– цепи, по которым передается видеосигнал от видеоадаптера до электродов электронно-лучевой трубки монитора;

– цепи, формирующие шину данных системной шины компьютера;

– цепи, формирующие шину данных внутри микропроцессора, и т.д.

Соответственно неинформативными ПЭМИН являются излучения, формируемые следующими цепями:

– цепи формирования и передачи сигналов синхронизации;

– цепи, формирующие шину управления и шину адреса системной шины;

– цепи, передающие сигналы аппаратных прерываний;

– внутренние цепи блока питания компьютера и т.д.

Расчет экрана электромагнитного излучения. Экранирование – локализация электромагнитной энергии в определенном пространстве с помощью экранирующих или поглощающих материалов.

В зависимости от назначения различают экраны с внутренним возбуждением электромагнитного поля, в которых обычно помещается источник помех, и экраны внешнего электромагнитного поля, во внутренней полости которых помещаются чувствительные к этим полям устройства. В первом случае экран предназначен для локализации поля в некотором объеме, во втором – для защиты от воздействия внешних полей.

Экран, защищая цепи, детали, колебательные контуры от воздействия внешних полей, оказывает существенной влияние на параметры экранируемых элементов. Из-за перераспределения электромагнитного поля внутри экрана происходят изменения их первичных параметров, в результате чего, например, изменяются магнитные связи, уменьшается первичная индуктивность катушек, увеличивается емкость контуров, возрастает активное сопротивление, что ведет к изменению частоты.

Экранирование с использованием вихревых токов обеспечивает одновременное ослабление как магнитных, так и электрических полей. Это дает основание такой способ экранирования называть электромагнитным. Эффективность экранирования такого экрана в ближней зоне (зоне индукции) будет не одинакова для составляющих поля. Поэтому, как правило, для ближней зоны следует вычислять каждый из компонентов поля в отдельности, принимая во внимание при этом, что в дальней зоне (зоне излучения) эффективности экранирования составляющих окажутся одинаковыми.

Физическая сущность электромагнитного экранирования, рассматриваемая с точки зрения теории электромагнитного поля и теории электрических цепей, сводится к тому, что под действием источника электромагнитной энергии на стороне экрана, обращенной к источнику, возникают заряды, а в его стенках – токи, поля которых во внешнем пространстве по интенсивности близки к полю источника, а по направлению противоположны ему и поэтому происходит взаимная компенсация полей. Такое рассмотрение представляется упрощенным, так как природа электромагнитного экранирования гораздо сложнее.

С точки зрения волновых представлений эффект экранирования проявляется из-за многократного отражения электромагнитных волн от поверхности экрана и затухания энергии волн по толщине. Отражение электромагнитной энергии обусловлено несоответствием волновых характеристик диэлектрика, в котором расположен экран и свойств материала экрана. Чем больше это несоответствие, чем больше отличаются волновые сопротивления экрана и диэлектрика, тем интенсивнее частичный эффект экранирования, определяемый отражением электромагнитных волн.

Эффективность электрически замкнутого экрана, т.е. способного ограничивать проникновение силовых линий электрического поля вне и внутри экранируемого пространства, определяется формулой:

$$Э_о = Э_{отр} \cdot Э_{погл} \cdot Э_{вн.отр}, \qquad (6.1)$$

где $Э_{отр}$ – ослабление энергии падающих волн за счет отражения на границе сред,

$Э_{погл}$ – ослабление вследствие затухания энергии в толще экрана,

$Э_{вн.отр}$ – ослабление из-за внутренних отражений в самом экране.

Обычно, если $Э_{погл} \geq 10$ дБ, то $Э_{вн.отр} = 1$, поэтому этой составляющей можно пренебречь, и тогда:

$$Э_о = Э_{отр} \cdot Э_{погл}, \qquad (6.2)$$

или в децибелах:

$$Э_о = 20 \cdot \lg(Э_{отр}) + 20\lg(Э_{погл}), \qquad (6.3)$$

Расчет электромагнитных экранов с достаточной точностью возможен только в некоторых в идеализированных случаях. К ним относятся:

1. Бесконечно плоский экран на пути распространения плоской волны;

2. Размещение точечного источника в центре герметичного идеального проводящего экрана сферической формы;

3. Бесконечно длинный идеально проводящий цилиндр с излучателем в виде бесконечной нити, расположенной на оси этого цилиндра.

Все эти случаи не отражают реальных условий работы экрана, поскольку не учитывают соотношения между длиной волны и линейными размерами экрана, характера источника, неравномерности распределения поля внутри экрана, неоднородности материала и конструкции самого экрана и главным образом возможности проникновения поля через щели и отверстия, имеющиеся в экране.

Однако выше перечисленные случаи позволяют получить многие общие зависимости, например, при падении плоской волны на плоский бесконечный экран. В этом случае величины потерь на отражение и поглощение определяются одинаково, т.к. в толще материала экрана как падающая, так и отраженная волны рассматриваются как плоские.

В металле электромагнитная волна затухает по экспоненциальному закону. Мерой скорости этого процесса является глубина проникновения волны или толщина поверхностного слоя δ. При прохождении волны через толщину поверхностного слоя δ она ослабевает в е раз. Если же толщина материала будет равной δ, она будет ослабевать в $e^{d/\delta}$ раз. Тогда:

$$Э_{погл} = 8{,}7 \cdot \frac{d}{\delta}, \qquad (6.4)$$

где d – толщина материала экрана, м.

Глубина проникновения представляет собой постоянную величину, характеризующую материал экрана и зависящую от частоты:

$$\delta = 0{,}03 \cdot \sqrt{\frac{\lambda \cdot \rho}{\mu_r}} = 0{,}52 \cdot \sqrt{\frac{\rho}{\mu_r \cdot f}}, \qquad (6.5)$$

где ρ - удельное сопротивление материала экрана, $\frac{Ом \cdot мм^2}{м}$,

λ - длина волны в воздушном пространстве, м,

f – частота, МГц,

μ_r – относительная магнитная проницаемость материала экрана,

δ - толщина поверхностного слоя, м.

На частотах 0,1 1 кГц экранирование вихревыми токами действует слабо и магнитное поле можно ослабить только шунтированием его ферромагнитным материалом с большим μ. С повышением частоты увеличивается вытеснение магнитного поля из объема ферромагнитного материала вследствие поверхностного эффекта, уменьшается действующая толщина экрана и эффективность экранирования шунтированием поля падает,

а с вытеснением поля растет. В диапазоне частот 0,1 – 1,0 кГц экранирование магнитного поля является труднейшей задачей и к нему прибегают крайне редко.

6.2 Практические задания

Задание 6.2.1. Рассчитать эффективность поглощения и глубину проникновения электромагнитного поля в экраны ЭМИ, выполненные из материалов, описанных в таблице 6.2. Толщина каждого из экранов составляет 3 мм.

Расчет произвести на десяти частотах диапазона 100 – 1000 МГц, взятых с шагом 100 МГц.

Задание 6.2.2. Построить в одной системе координат частотные зависимости эффективности поглощения ЭМИ каждым из рассчитанных экранов.

Задание 6.2.3. Сделать вывод об эффективности использования каждого из рассчитанных экранов в заданном частотном диапазоне.

Таблица 6.2 – Характеристики некоторых металлов

Металл	Удельное сопротивление $\frac{Ом \cdot мм^2}{м}$	μ
Медь	0,0175	1
Латунь	0,06	1
Алюминий	0,03	1
Сталь	0,1	200
Пермаллой	0,65	12000

6.3 Контрольные вопросы

1. В чем смысл Soft Tempest технологии?
2. Что называют эффективностью экранирования ЭМИ?
3. Какие блоки ПК являются источниками опасного ЭМИ?
4. В чем заключается физический смысл глубины проникновения ЭМИ?
5. Каким образом может произойти утечка информации через порты ПК?
6. Каково назначение экранов ЭМИ?
7. Какие различают разновидности экранов ЭМИ?
8. Какие требования предъявляются к экранам ЭМИ?
9. Какие механизмы имеют место при взаимодействии ЭМИ с экраном?
10. С использованием каких формул производится оценка эффективности электромагнитного экранирования?