УДК: 621.394.6

А.А. Хорев

Оценка возможности обнаружения побочных электромагнитных излучений видеосистемы компьютера

Рассмотрены вопросы, связанные с перехватом побочных электромагнитных излучений (ПЭМИ), возникающих при выводе изображения на экран монитора, оптимальным приемником. Предложены математическая модель и методика оценки возможностей перехвата ПЭМИ видеосистемы компьютера техническими средствами разведки (ТСР).

Ключевые слова: видеосистема, побочные электромагнитные излучения, технический канал утечки информации, перехват информации.

К одной из основных угроз безопасности информации ограниченного доступа, обрабатываемой техническими средствами (ТС), относится *утечка информации по техническим каналам*, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего перехват информации.

При обработке информации ПЭВМ технические каналы утечки информации образуются за счет побочных электромагнитных излучений (ПЭМИ), а также вследствие наводок информационных сигналов в линиях электропитания ПЭВМ, соединительных линиях вспомогательных технических средств и систем, цепях заземления и посторонних проводниках.

Наиболее опасным (с точки зрения утечки информации) режимом работы ПЭВМ является вывод информации на экран монитора.

Исследования по перехвату побочных электромагнитных излучений (ПЭМИ) видеомониторов ПЭВМ начались практически одновременно с их созданием и носили закрытый характер.

В зарубежной литературе вместо термина ПЭМИ используются термины «compromising electromagnetic emanations» (компрометирующие электромагнитные излучения) или TEMPEST (сокращение от «transient electromagnetic pulse emanation standard» – стандарт на электромагнитные импульсные излучения, вызванные переходными процессами в электронной аппаратуре).

Первые открытые публикации по перехвату ПЭМИ ПЭВМ появились в начале 80-х годов прошлого века. Наибольшее внимание из них привлекла статья голландского ученого Вима Ван Эйка (Wim van Eck) «Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?», опубликованная в журнале «Computers and Security» в декабре 1985 г. [1].

С тех пор многое изменилось. Переход на интерфейсы VGA и DVI значительно усложнил задачу перехвата ПЭМИ.

Наиболее подробно исследование проблемы перехвата ПЭМИ видеомониторов с интерфейсами VGA и DVI проведено в диссертации М.Г. Кюн (Markus G. Kuhn)) [2]. Для перехвата ПЭМИ он использовал цифровой супергетеродинный приемник Dynamic Sciences R1250 с логопериодической антенной.

Сигнал с демодулятора приемника подавался на цифровой запоминающий осциллограф Tektronix TDS 7054, а затем обрабатывался с использованием специального программного обеспечения и преобразовывался в растровые изображения, которые выводились на монитор компьютера в реальном масштабе времени. Для синхронизации изображения использовался внешний высокостабильный генератор импульсов R-1160C.

Эксперименты проводились в здании, расположенном в полугородской среде. Несмотря на то, что в здании находилось более 100 работающих компьютеров, при экспериментах удавалось перехватывать текстовые изображения на расстояниях 10 м через два офисных помещения (три гипсокартонные стены), расположенных на том же этаже здания [2].

Использование цифрового запоминающего осциллографа позволило М.Г. Кюну реализовать метод некогерентного накопления импульсов, что существенно повысило качество перехваченных изображений. Время усреднения (количество усредняемых кадров) ограничивалось памятью цифрового запоминающего осциллографа.

При проведении исследований М.Г. Кюн установил, что частота обновления яркости (цвета) каждого пикселя изображения F_n (*pixel clock frequency*) зависит от размеров изображения, частоты обновления экрана $F_к$ и особенностей видеокарты, что позволяет, «подстроившись» под тактовую частоту F_n конкретного компьютера, выделять изображение, выводимое на экран его монитора, на фоне побочных электромагнитных излучений других компьютеров.

В открытой отечественной литературе публикации, связанные с техническими каналами утечки информации, вызванными побочными электромагнитными излучениями, стали появляться в конце прошлого – начале этого века. Основное внимание в этих работах уделено средствам измерений и методам измерений ПЭМИ в целях оценки эффективности защиты средств вычислительной техники от утечки информации по техническим каналам, однако вопросы, связанные с теоретической оценкой возможностей перехвата ПЭМИ средствами разведки, практически не рассматривались.

Целью данной статьи является разработка математической модели обнаружения побочных электромагнитных излучений видеосистемы компьютера оптимальным приемником, позволяющей проводить оценку возможностей перехвата ПЭМИ средствами разведки.

Проведенный анализ показал, что в качестве показателя оценки возможности перехвата ПЭМИ СВТ наиболее часто используется вероятность правильного обнаружения информативного сигнала приемным устройством средства разведки P_O при фиксированной ложной тревоге $P_{лт}$ (критерий Неймана–Пирсона).

При перехвате изображения, выводимого на экран монитора, необходимо учитывать, что оно стабильно в течение некоторого времени (T_a), которое зависит от характера действий оператора ПЭВМ и может варьировать от нескольких секунд (при наборе текста) до нескольких минут (при чтении текста). Данный факт позволяет использовать методы цифровой корреляционной обработки принимаемых импульсных сигналов, что существенно повышает отношение сигнал/шум. Следовательно, для расчета вероятности правильного обнаружения пачки одинаковых слабых некогерентных нефлюктуирующих импульсов можно использовать формулу [3]

$$P_O \approx \Phi\left(q \cdot \sqrt{N} - \Phi^{-1}\left(1 - P_{\text{лт}}\right)\right), \tag{1}$$

где $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} \exp\left(-\frac{t^2}{2}\right) dt$ – интеграл вероятности; $\Phi^{-1}(x)$ – функция, обратная $\Phi(x)$;

q – энергетическое отношение сигнал/шум на входе разведывательного приемника; N – количество осредненных импульсов, $N = F_{\text{к}} \cdot T_a$; $F_{\text{к}}$ – частота кадровой развертки монитора, Гц; T_a – время стабильности перехватываемого изображения, с.

Учитывая, что для оптимального приемника полоса пропускания фильтра $\Delta F = 1/\tau$, и допуская, что форма импульса прямоугольная, энергетическое отношение сигнал/шум на входе разведывательного приемника q будет равно

$$q = \frac{P_{\text{и}}}{N_{\text{ш}}}, \tag{2}$$

где $P_{\text{и}}$ – мощность одиночного импульса на входе разведывательного приемника, Вт; $N_{\text{ш}}$ – мощность шума, приведенная ко входу разведывательного приемника в полосе пропускания ΔF, Вт.

Мощность шума, приведенная к входу разведывательного приемника, будет определяться как собственными шумами приемника, так и шумами антенны

$$N_{\text{ш}} = \sqrt{N_{\text{ш.п}}^2 + N_{\text{ш.а}}^2}, \tag{3}$$

где $N_{\text{ш.п}} = \int\limits_{\Delta F} N_{\text{ш.п}}(f) df$ – мощность собственных шумов приемника в полосе пропускания ΔF; $N_{\text{о.п}}(f)$ – спектральная плотность мощности собственных шумов приемника; $N_{\text{ш.а}} = \int\limits_{\Delta F} N_{\text{ш.а}}(f) df$ – мощность шумов антенны, приведенная ко входу разведывательного приемника в полосе пропускания ΔF; $N_{\text{ш.а}}(f)$ – спектральная плотность мощности шумов антенны, приведенная ко входу разведывательного приемника.

Из-за большого количества случайных факторов рассчитать мощность ПЭМИ не представляется возможным. Поэтому оценку возможностей по перехвату ПЭМИ для каждой ПЭВМ проводят инструментально-расчетным методом, предполагающим изменение уровней напряженности поля ПЭМИ на расстоянии d = 1 м и измерение или расчет затухания сигнала на трассе «ПЭВМ – средство разведки» (рис. 1).

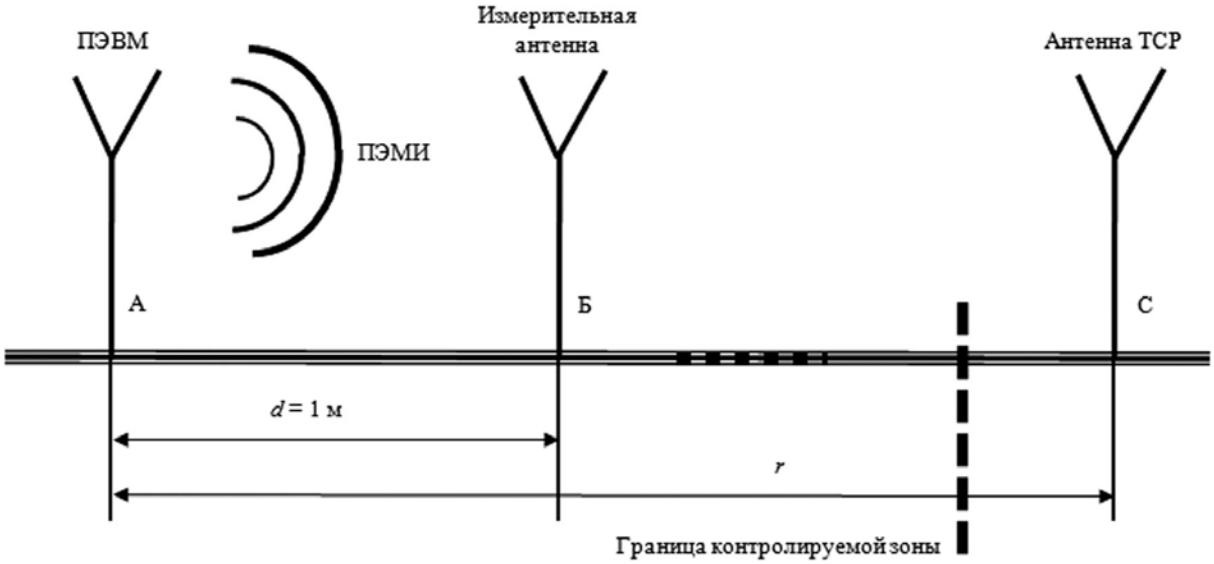

Рис. 1. Схема расчетно-инструментального метода оценки защищенности ПЭВМ от утечки информации, возникающей за счет ПЭМИ

Учитывая, что при выводе на экран монитора реального изображения побочные электромагнитные излучения видеосистемы ПЭВМ анализатором спектра не обнаруживаются, измерения рекомендуется проводить при выводе на экран монитора тестового сигнала «точка – через точку», представляющего собой чередование «белых» и «черных» пикселей.

При таком виде тестового изображения спектр ПЭМИ носит дискретный характер, уровень излучаемых ПЭМИ максимален.

Например, проведенные исследования ПЭМИ ПЭВМ с интегрированной видеокартой Intel (R) HD Graphis Family с интерфейсом VGA [4] показали, что для теста «точка – через точку» для разрешения монитора 1280×1024×60:

– спектральные составляющие ПЭМИ видеосистемы ПЭВМ выявлены в диапазоне частот от 54 до 2322 МГц (вплоть до 43-й гармоники);

– частота первой гармоники ПЭМИ составляет: $F_{\text{с}} = F_{\text{п}}/2 \approx 54$ МГц, где $F_{\text{п}}$ – частота обновления яркости (цвета) каждого пикселя;

– длительность импульсов цветности $\tau \approx 8{,}95$ нс ($\tau \approx 0{,}97/ F_{\text{п}}$), а и их период следования $T \approx 18{,}6$ нс (т.е. $Q = T/\tau \approx 2$).

Учитывая, что наиболее вероятно роль случайных антенн при излучении ПЭМИ выполняют проводники, соединяющие выход цифроаналогового преобразователя видеоадаптера с разъемом VGA, и кабель, соединяющий системный блок с монитором, будем полагать, что в излучении ПЭМИ доминирует электрическая составляющая электромагнитного поля $E_{\text{с}}$.

Уровни напряженности поля информативных сигналов ПЭМИ измеряются на всех обнаруженных частотах f_i в режиме среднеквадратичного детектора (RMS) при включенном и выключенном тесте.

С учетом погрешностей измерений максимально возможный уровень напряженности поля информативного сигнала ПЭМИ за период измерений рассчитывается по формуле

$$E_{\text{с}.i} = \sqrt{(\varepsilon_{\text{и}} E_{\text{и}.i})^2 - (E_{\text{п}.i}/\varepsilon_{\text{и}})^2}\ , \qquad (4)$$

где $E_{\text{с}.i}$ – максимально возможный уровень напряженности поля информативного сигнала ПЭМИ за период измерений на i-й частоте, мкВ/м; $E_{\text{и}.i}$ – измеренное значение напряженности поля информативного сигнала ПЭМИ на i-й частоте при включенном тесте, мкВ/м; $E_{\text{п}.i}$ – измеренное

значение напряженности поля на i-й частоте при выключенном тесте, мкВ/м; $\varepsilon_{\text{и}} = 1 + \sqrt{\left(10^{0{,}05\cdot\varepsilon_a} - 1\right)^2 + \left(10^{0{,}05\cdot\varepsilon_{\text{ип}}} - 1\right)^2}$ – среднеквадратическая погрешность измерительного тракта; ε_a – среднеквадратическая ошибка калибровки измерительной антенны, дБ; $\varepsilon_{\text{ип}}$ – среднеквадратическая ошибка измерения амплитуды сигнала измерительным приемником, дБ.

Измерив напряженность электромагнитного поля информативных составляющих ПЭМИ $E_{c.i}$ и полагая, что полоса пропускания входного фильтра $\Delta F = 1/\tau$, отношение сигнал/шум на входе разведывательного приемника для каждого частотного диапазона, в котором обнаружены информативные составляющие ПЭМИ, можно рассчитать по формуле

$$q_j = \frac{Q\cdot U_{\text{с}.j}^2/Z}{\sqrt{N_{\text{ш.п}.j}^2 + N_{\text{ш.а}.j}^2}} \approx \frac{2\cdot\sum\limits_{\Delta F_j}\left(\dfrac{E_{\text{с}.i}}{K_{\text{а}.i}\cdot V_{r.i}}\right)^2}{Z\cdot\sqrt{\left(\sum\limits_{m=1}^{M_j} N_{\text{о}.j.m}(f)\cdot\Delta F_{\text{и}}\right)^2 + \left(\sum\limits_{m=1}^{M_j}\dfrac{\left(E_{\text{ш.а}.j.m}(f)/K_{a.j.m}(f)\right)^2}{Z}\cdot\Delta F_{\text{и}}\right)^2}}, \qquad (5)$$

где $E_{\text{с}.i}$ – напряженность электрической составляющей электромагнитного поля i-й спектральной составляющей, входящей в состав j-го частотного интервала, В/м; $K_{\text{а}}(f)$ – спектральный калибровочный коэффициент антенны средства разведки, 1/м; $K_{\text{а}.i}$ – значение калибровочного коэффициента антенны средства разведки на i-й частоте, 1/м; $V_{r.i}$ – коэффициент ослабления сигнала на i-й частоте на трассе «ПЭВМ – средство разведки»; ΔF_j – j-й частотный интервал; $E_{\text{ш.а}.n}(f)$ – спектральная чувствительность антенны, измеренная на m-й частоте, входящей в состав j-го частотного интервала, при отношении сигнал/шум $q = 1$, В/(м$\cdot\sqrt{\text{Гц}}$); $N_{\text{о}.n}(f)$ – спектральная плотность мощности собственных шумов приемного устройства, измеренная на m-й частоте, входящей в состав j-го частотного интервала, В/(м$\cdot\sqrt{\text{Гц}}$); $\Delta F_{\text{и}}$ – ширина полосы пропускания измерительного приемника при измерении $E_{\text{с}.i}$, Гц; $M_j \approx \Delta F_j/\Delta F_{\text{и}}$; $Q = T/\tau$ – скважность тестового сигнала (при тесте «точка – через точку» $Q \approx 2$); T – период следования пиксельных импульсов, с; τ – длительность пиксельных импульсов, с; Z – входное сопротивление приемного устройства, Ом.

Расчет значений граничных частот частотных интервалов ΔF_j осуществляется по формулам

$$\Delta F_j = f_{\text{в}.j} - f_{\text{н}.j} = \Delta F; \quad f_{\text{н}j} = \frac{10^{-6}(j-1))}{\tau}; \quad f_{\text{в}j} = \frac{10^{-6}\cdot j}{\tau}, \qquad (6)$$

где $f_{\text{н}j}$ – нижняя частота j-го частотного интервала, МГц; $f_{\text{в}j}$ – верхняя частота j-го частотного интервала, МГц; τ – длительность импульсов передачи оттенка цвета в тестовом режиме, с.

Полагая, что шумы антенны значительно выше собственных шумов приемного устройства средства разведки, формулу (5) запишем в виде

$$q_j \approx \frac{2\cdot\sum\limits_{\Delta F_j}\left(\dfrac{E_{\text{с}.i}}{K_{\text{а}.i}\cdot V_{r.i}}\right)^2}{Z\cdot\sum\limits_{m=1}^{M_j}\dfrac{\left(E_{\text{ш.а}.j.m}(f)/K_{\text{а}.j.m}(f)\right)^2}{Z}\cdot\Delta F_{\text{и}}} \approx \frac{2\cdot n_j}{\Delta F_j}\cdot\sum_{\Delta F_j}\left(\frac{E_{c.i}}{E_{\text{ш.а}.i}\cdot V_{r.i}}\right)^2, \qquad (7)$$

где $E_{\text{с}.i}$ – напряженность электрической составляющей электромагнитного поля i-й спектральной составляющей, входящей в состав j-го частотного интервала, мкВ/м; $V_{r.i}$ – коэффициент ослабления сигнала на i-й частоте на трассе «ПЭВМ – средство разведки»; $E_{\text{ш.а}.i}$ – спектральная чувствительность антенны на i-й частоте, измеренная при отношении сигнал/шум $q = 1$ и $\Delta F = 1$ Гц, мкВ/(м$\cdot\sqrt{\text{Гц}}$); ΔF_j – j-й частотный интервал, Гц; n_j – количество измеренных спектральных составляющих, попадающих в j-й частотный интервал.

При измерении уровней напряженности поля сигналов ПЭМИ в зависимости от длины волны измерительная антенна может оказаться в ближней, средней или дальней зонах. Ближняя зона ограничена расстоянием от излучателя $r \le \lambda/2\pi$. Дальняя зона начинается с расстояния $r > (3...10)\lambda$. Будем полагать, что границей дальней зоны является расстояние $r = 6\lambda$.

В ближней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально кубу расстояния (~ $1/r^3$), а дальней – обратно пропорционально расстоянию (~ $1/r$). Предположим, что в средней зоне электрическая составляющая электромагнитного поля E_c убывает обратно пропорционально квадрату расстояния (~ $1/r^2$).

Тогда затухание на трассе «ПЭВМ – средство разведки» V_r (безразмерная величина) можно рассчитать по формулам [5]:

А. Для частоты сигнала ПЭМИ ниже $f \le 47{,}75$ МГц

$$V_r \approx \begin{cases} r^3 \quad \text{если} \quad r \le \dfrac{47{,}75}{f}; \\ \dfrac{47{,}75 \cdot r^2}{f} \quad \text{если} \quad \dfrac{47{,}75}{f} < r \le \dfrac{1800}{f}; \\ \dfrac{8{,}59 \cdot 10^4 \cdot r}{f^2} \quad \text{если} \quad r > \dfrac{1800}{f}. \end{cases} \tag{8}$$

Б. Для частоты сигнала ПЭМИ $47{,}75 \text{ МГц} < f \le 1800$ МГц

$$V_r \approx \begin{cases} r^2 \quad \text{если} \quad r \le \dfrac{1800}{f}; \\ \dfrac{1800 \cdot r}{f} \quad \text{если} \quad r > \dfrac{1800}{f}. \end{cases} \tag{9}$$

В. Для частоты сигнала ПЭМИ $f > 1800$ МГц

$$V_r \approx r, \tag{10}$$

где f – частота измеренного сигнала, МГц; r – расстояние от ПЭВМ до средства разведки, м.

Выбор нормативного (порогового) значения вероятности правильного обнаружения сигнала целесообразно осуществлять с точки зрения минимизации вероятности полной ошибки $P_{\text{ош}}$.

Проведенный анализ показал, что при априорной вероятности появления сигнала $P^* = 0{,}5$ значения вероятностей полной ошибки $P_{\text{ош}}$ значительно превышают значения вероятностей правильного обнаружения сигнала $P_{\text{о}}$ ($P_{\text{ош}} >> P_{\text{о}}$) при $P_{\text{о}} < 0{,}05$, становятся соизмеримы с ними ($P_{\text{ош}} \approx P_o$) при $P_{\text{о}} \approx 0{,}33 \cdot (1 + P_{\text{лт}})$ и становятся значительно их меньше ($P_{\text{ош}} << P_{\text{о}}$) при $P_{\text{о}} > 0{,}83 \cdot (1 + P_{\text{лт}})$ [6].

Случай, когда вероятность ошибки соизмерима с вероятностью правильного обнаружения сигнала, является случаем наибольшей неопределённости при принятии решения о наличии или отсутствии сигнала. Поэтому в качестве порогового значения *при решении задачи обнаружения сигнала* целесообразно принять значение вероятности правильного обнаружения $P_n \approx 0{,}3$.

Задаваясь пороговыми значениями вероятности правильного обнаружения сигнала P_n и вероятности ложной тревоги $P_{\text{лт}}$ из формулы (1) легко получить предельно допустимое (пороговое) значение энергетического отношения сигнал/шум на входе приёмного устройства средства разведки δ

$$\delta \approx \frac{\Phi^{-1}(P_n) + \Phi^{-1}(1 - P_{\text{лт}})}{\sqrt{N}}. \tag{11}$$

Например, для вероятностей $P_n = 0{,}3$ и $P_{\text{лт}} = 10^{-3}$ пороговое значение отношения сигнал/шум на входе приёмного устройства средства разведки будет равно $\delta \approx 2{,}68/\sqrt{N} = 2{,}68/\sqrt{F_{\text{к}} \cdot T_{\text{а}}}$.

Пространство вокруг ПЭВМ, в пределах которого отношение сигнал/шум q на входе разведывательного приемника превышает пороговое значение δ ($q \ge \delta$), называется *опасной зоной* 2 ($R2$). Следовательно, перехват ПЭМИ ПЭВМ возможен при выполнении двух условий (рис. 2 [6]):

– первое – расстояние от ПЭВМ до границы контролируемой зоны должно быть менее зоны $R2$ ($R_{\text{кз}} \le R2$);

– второе – в пределах зоны $R2$ возможно размещение средств разведки ПЭМИН.

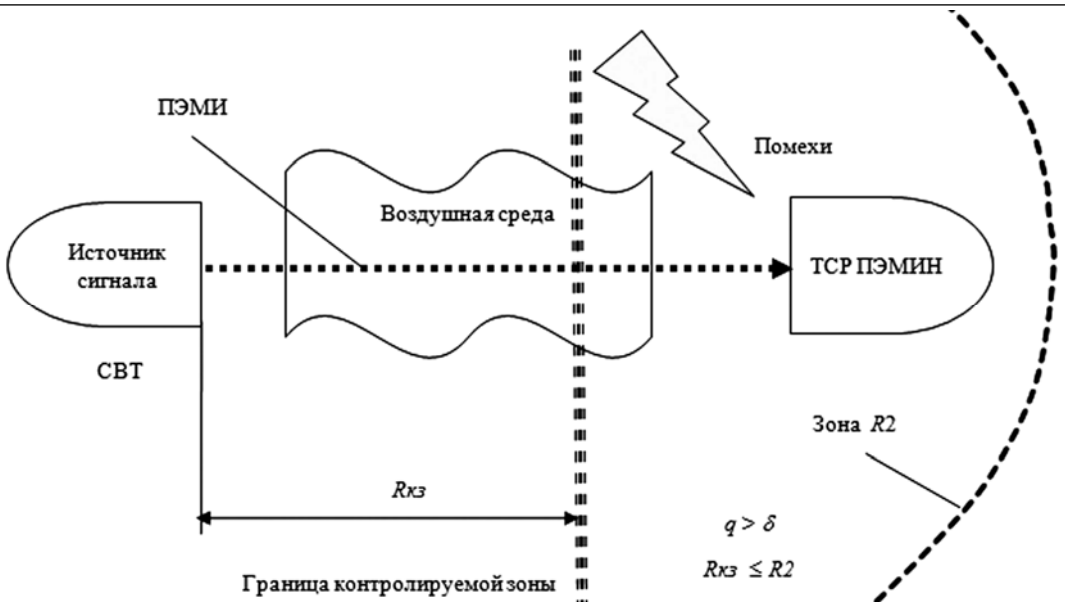

Рис. 2. Схема перехвата побочных электромагнитных излучений ПЭВМ (электромагнитный технический канал утечки информации)

Обычно зону $R2$ рассчитывают применительно к стационарным, перевозимым и переносимым средствам разведки.

Расчет зоны $R2$ проводится в следующей последовательности.

Начиная с расстояния $r = 1$ м с шагом 1 или 5 м по формуле (5) или (7) рассчитывается отношение сигнал/шум q_j для каждого частотного диапазона, в котором обнаружены информативные составляющие ПЭМИ. Полученные значения q_j сравниваются с рассчитанным по формуле (11) пороговым отношением сигнал/шум δ. За значение зоны $R2$, м, принимается то минимальное расстояние r, при котором для всех частотных диапазонов выполняется условие $q_j \le \delta$, т.е. $R2 = \min\{r\} | q_j \le \delta$.

Таким образом, предложенная математическая модель обнаружения побочных электромагнитных излучений видеосистемы компьютера оптимальным приемником позволяет оценить возможность перехвата ПЭМИ ПЭВМ средствами разведки и обосновать целесообразность использования на объектах информатизации тех или иных технических средств защиты информации.

Литература

1. Wim van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? [Электронный ресурс]. – Режим доступа: http://cryptome.org/emr.pdf, свободный (дата обращения: 03.12.2013 г.).

2. Kuhn G. Compromising emanations: eavesdropping risks of computer displays: This technical report is based on a dissertation submitted June 2002 by the author for the degree of Doctor of Philosophy to the University of Cambridge, Wolfson College. [Электронный ресурс]. – Режим доступа: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf, свободный (дата обращения: 03.12.2013 г.).

3. Теоретические основы радиолокации: учеб. пособие для вузов. – 2-е изд., перераб. и доп. / А.А. Коростылев, Н.Ф. Клюев, Ю.А. Мельник и др. / Под ред. В.Е. Дулевича. – М.: Сов. радио, 1978. – 608 с.

4. Исследование побочных электромагнитных излучений видеосистем средств вычислительной техники. Шифр «107-ИПП-ИБ»: отчет о НИР «заключ.» / МИЭТ; рук. А.А. Хорев – М., 2013. – 167 с.

5. Хорев А.А. Оценка возможности по перехвату побочных электромагнитных излучений видеосистемы компьютера. Ч. 2 // Специальная техника. – 2011. – № 4. – С. 51–62.

6. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов: в 3 т. – Т. 1: Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

Хорев Анатолий Анатольевич
Д-р техн. наук, профессор, зав. каф. «Информационная безопасность»
Национального исследовательского университета «МИЭТ», Москва
Тел.: 8-916-500-01-64
Эл. почта: horev@miee.ru

Horev A.A.
Evaluation of the possibility of detection side compromising electromagnetic emanations video PC

One of the most dangerous channels of the leakage of information with restricted access, on-cultivated PC channel is the leakage arising from side within the compromising electromagnetic emanations video PC. In the article development of a mathematical model for discovering compromising electromagnetic emanations video PC optimal receiver and instrumental calculation method for evaluation of power interception compromising electromagnetic emanations means of intelligence. Developed the mathematical model takes into account the possibility of improving the signal to noise due to digital signal processing with the interception of multiple «frames» image.
Keywords: video system, compromising electromagnetic emanations, technical channel of information leakage, the interception of information.