4. Hayes I.F. Modeling and Analysis of Computer Cammunications Networks, N-Y, 1984.

5. Гермейер Ю.Б. Введение в теорию исследования операций. М. "Наука", 1971.

6. Хоменюк В.Б. Элементы теории многоцелевой оптимизации. М. "Наука", 1983.

7. Arrow K.J. Rational choice functions and orderings. Econometrica. 1959, vol.26, p.121-127.

8. Sen A.K. Choice functions and revealed preference. Rev. Econ. Stud. , 1971, vol. 38, p. 307-317.

9. Нэш Д. Бескаалиционные игры. В кн.: Матричные игры. М., Физматиз, 1961.

10. Milnor J. Games against nature. In: Decision processes., 1954.

11. Arrow K.J. Hurwicz Y. An optimality criterion for decisionmaking under ignorance. In: Uncertainty and expectation in economics. Oxford, 1977

12. Дружинин В.В. , Конторов Д.С. , Конторов М.Д. Введение в теорию конфликта., М. "Радио и связь", 1989.

13. Подиновский В.Б., Нагин В.Д. Парето-оптимальные решения многокритериальных задач М. "Наука", 1982

Надійшла 14.01.2002
Після доработки 27.02.2002

УДК 681.3

Анкудович Г.Г., Катерноза К.А.

АНАЛИТИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ СИГНАЛОВ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВОДОК ЭЛЕМЕНТОВ ЛВС АИС ГНС УКРАИНЫ.

Анализ состояния дел в области защиты информации показывает, что в промышленно развитых странах мира уже сложилась вполне оформившаяся инфраструктура защиты информации (ЗИ) в системах обработки данных. И тем не менее, количество фактов злоумышленных действий над информацией не только не уменьшается, но и имеет достаточно устойчивую тенденцию к росту. В этом смысле Украина не является, к сожалению, исключением.

Среди всех возможных каналов утечки информации наибольшую опасность в Украине в ближайшее время, очевидно, будут представлять технические каналы. Такое представление основывается на следующих факторах:

- наличие в Украине большого числа технически грамотных специалистов, знания и навыки которых не востребованы вследствие тяжелого экономического положения;
- выход на украинский рынок фирм других стран – производителей аппаратуры для технического шпионажа;
- недостаточное внимание, а чаще всего просто игнорирование проблем безопасности информации со стороны руководящего состава министерств, ведомств и организаций.

Сегодня уже ни для кого не секрет, что наряду с такими «обычными» техническими каналами утечки информации, как установка радиомикрофонов, подключение к телефонной линии связи, акустическое подслушивание, дистанционное фотографирование и т.д., существует ещё и радиотехнический канал утечки информации из средств вычислительной техники.

Проблема утечки информации из вычислительной техники через побочные электромагнитные излучения и наводки (ПЭМИН) известна уже давно. Однако

актуальной она стала в последние несколько лет. Это связано как с широчайшим распространением персональных компьютеров (ПК), так и с созданием разветвленной сети автоматизированных информационных систем сбора, обработки, хранения и передачи различного рода информации в интересах того или иного ведомства.

В настоящее время технические средства радиоэлектронного перехвата и средства несанкционированного доступа к информационным структурам и информационным ресурсам по своим техническим возможностям значительно опережают средства информационной защиты. В современных зарубежных средствах разведки используются супертехнологии, позволяющие произвести обнаружение и детальный сигнатурный анализ ПЭМИН персональных компьютеров, локальных вычислительных сетей, различного рода закладных устройств с расстояний, значительно превышающих границы зоны безопасности информации, определенные руководящими документами.

В средствах радиотехнического перехвата США применяются высокочастотные фильтры с высокотемпературной сверхпроводимостью (до 77° К) [1]. Набор таких сверхузкополосных фильтров (до 100 в поддиапазоне одновременного анализа) образует многоканальный разведывательный приёмник – спектроанализатор, подключенный непосредственно к приёмной антенне. Спектроанализатор позволяет обнаружить, отселектировать и проанализировать не только основные, но и слабые побочные излучения радиотехнических систем, персональных компьютеров и других элементов вычислительной системы, линий связи на дальностях, в несколько раз превышающих дальность обнаружения сигналов штатной аппаратурой контроля радиоизлучений, применяемой в Украине.

Использование узкополосных фильтров позволяет отстроиться от узкополосных помех, создаваемых преднамеренно и непреднамеренно, и выделить строго заданные типы сигналов на фоне интенсивного потока мешающих излучений (телевидения, средств связи, излучения двигателей внутреннего сгорания и т.д.).

Применение таких технологий и совершенствование методов додетекторной и последетекторной обработки сигналов ставит серьёзные проблемы защиты конфиденциальной информации всех структур государственной системы, в том числе и государственной налоговой службы Украины. В этих условиях эффективной будет только хорошо организованная комплексная защита, основанная на научном подходе и рациональном построении системы противодействия несанкционированному доступу.

К сожалению, несмотря на большое количество структур, организаций, специалистов, занимающихся защитой информации, открытых публикаций по комплексному научному исследованию в этой области пока не просматривается. Наиболее весомые результаты достигнуты только в области криптографической защиты.

Разработанная техника контроля ПЭМИН измеряет только спектральную мощность побочного излучения спектроанализаторами с различными полосами избирательных фильтров (1; 3; 10; 30; 100; 300кГц). Точность измерения уровня ПЭМИН составляет порядка ±2%. Спектроанализатор, по существу, является энергетическим приёмником и характеризует только возможность несанкционированного обнаружения сигналов ПЭМИН. Но для получения смысловой информации злоумышленнику необходимо обеспечить структурную и информационную доступность, а владельцу информации необходимо обеспечить структурную и информационную скрытность от радиотехнического перехвата.

Структурная скрытность определяет способность противостояния раскрытию структуры сигналов (методов кодирования, закрытия информации) и характеризуется вероятностью правильного вскрытия структуры сигнала ($P_{вск}$).

Информационная скрытность характеризует способность противостоять мерам вскрытия смысловой информации по результатам перехвата побочных излучений. Для осуществления этих процедур злоумышленнику необходимо вскрыть не только

спектральную, но и временную структуру побочного излучения, как отдельной посылки (импульса), так и структуру импульсного потока излучений. Для этого потребуется обеспечить отношение сигнал/шум на 10..15дБ выше, чем при спектральном анализе. Для организации противодействия несанкционированному доступу необходимо также знать структуру электромагнитного поля во временной области, в первую очередь, структуру излучаемых импульсов, которая в значительной степени отличается от структуры информационных импульсов.

Информационный сигнал, циркулирующий в компьютерных сетях, представляет собой последовательность единиц и нулей. С точки зрения технической реализации символ «1» соответствует положительному импульсу, а символ «0» - отрицательному, т.е. в компьютерных сетях циркулирует дискретный сигнал. Однако, излучающие структуры компьютерной сети (элементы, цепи питания, соединительные линии, среда распространения) ближе к аналоговым звеньям. Поэтому в научном плане исследования реальной структуры сигнала ПЭМИН основное внимание следует уделить вопросам преобразования цифровых сигналов аналоговыми звеньями в сигналы электромагнитного поля в дальней зоне.

В первую очередь, для этого требуется теоретически обосновать природу ПЭМИН, их структуру во временной и спектральных областях за пределами корпуса ПК, помещения, здания, охраняемой зоны.

Вся классическая теория электромагнитного поля основана на синусоидальной структуре сигнала. В нашем случае первичным (исходным) источником формирования электромагнитного поля является цифровой сигнал (сигнал без несущей), который, по сути, является аналогом непрерывного секвентного сигнала.

Основная особенность в природе формирования и излучения сигнала в дальней зоне связана с требованием нулевого значения спектральной функции на нулевой частоте, т.е. отсутствия постоянной составляющей:

$$S(j\omega) = \int_{-\frac{\tau_u}{2}}^{\frac{\tau_u}{2}} S(t)\exp(-j\omega t)dt \Big/_{\omega=0} = \int_{-\frac{\tau_u}{2}}^{\frac{\tau_u}{2}} S(t)dt = 0, \qquad (1)$$

где $S(j\omega)$ – спектральная функция сигнала в дальней зоне;

$S(t)$ – временная функция сигнала;

τ_u - длительность импульса.

Физически условие (1) соответствует знакопеременности электромагнитного поля. Это требование справедливо для любых моделей сигналов: узкополосных, широкополосных и сверхширокополосных. Даже незначительный уровень постоянной составляющей только увеличивает нагрев ПК, т.к. затраченная энергия на тепло увеличивает шумы в цепях ПК.

В нашем случае несинусоидальный сигнал за счет изменения тока в цепях ПК в момент нарастания и спада амплитуды импульсов создает электромагнитное поле побочного излучения.

Таким образом, следует считать, что электромагнитный импульс побочного излучения создает сигнал, первая производная которого состоит из коротких положительных и отрицательных импульсов, созданных в цепях ПК во время переходного процесса (рис.1):

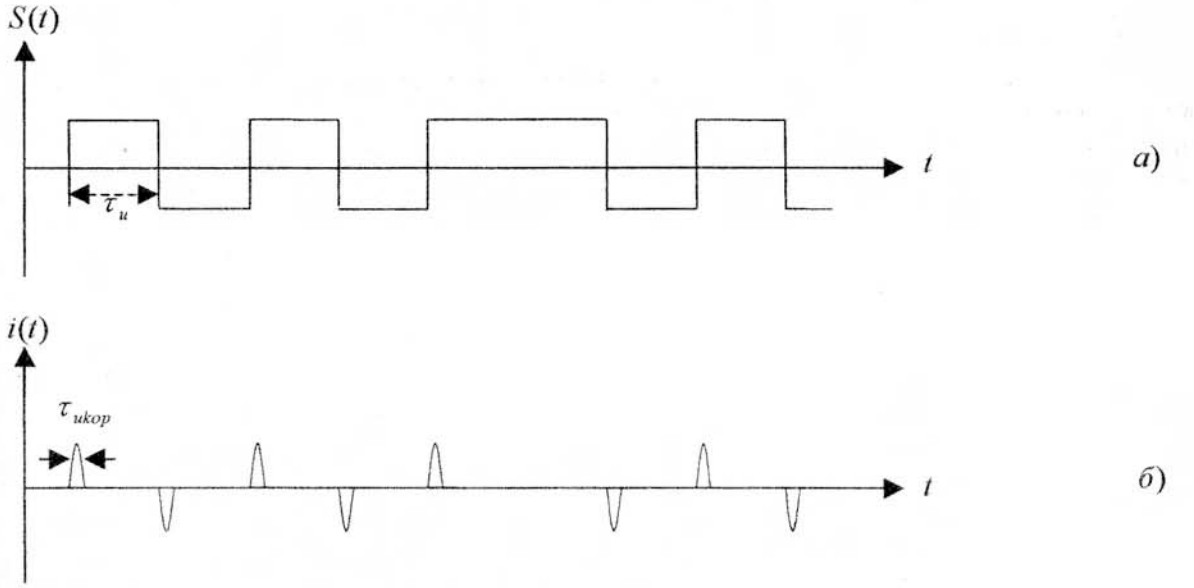

Рис. 1. Формирование побочного излучения,
где а) информационный импульс ПК;
б) импульсы тока.

Если допустить, что информационные импульсы имеют квазипрямоугольную форму с крутыми фронтами, то спектр одиночного импульса на выходе системы формирования импульса излучения будет определяться не длительностью информационного импульса (τ_u), а длительностью импульса тока ($\tau_{икор}$):

$$S(f) = \sqrt{2}\,\frac{\sin \pi f \dfrac{\tau_{икор}}{T_i}}{\pi f \dfrac{\tau_{икор}}{T_i}}, \qquad (2)$$

где T_i - период импульсной последовательности;

f - несущая частота.

Таким образом, можно считать, что время переключения сигнальной функции $S(t)$ определяет длительность излученного элементарного сигнала.

В зависимости от ширины эквивалентной полосы пропускания устройств, формирующих излученный сигнал, импульс электромагнитного поля в дальней зоне будет иметь колебательную структуру, т.е. излучаться будет финитный сигнал (рис.2):

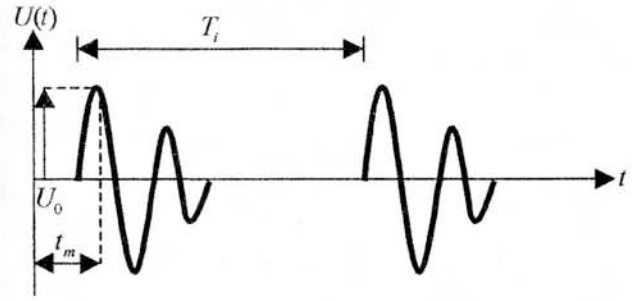

Рис. 2. Финитный сигнал электромагнитного поля

Экспериментально и теоретически доказано, что каждая информационная посылка содержит целое число периодов затухающих колебаний [2]. Это утверждение

вытекает из свойств электромагнитного поля – необходимости отсутствия постоянной составляющей.

Анализ решений уравнения Максвелла для возбуждающихся токов, приводящих к классу цифровых функций, показывает, что излучаемая мощность будет тем больше, чем больше среднее число символов при условии, что энергия положительных (+1) и отрицательных (-1) символов равна, а среднее значение возбуждающего тока также должно равняться нулю.

Круговую частоту заполнения импульсов затухающими колебаниями можно рассчитать по формуле [3]:

$$\omega = \omega_c \left(1 + \frac{\omega_c^2 - \alpha^2}{\omega_0^2 \omega_c^2 t - 4\omega_c^2 \alpha t + \omega_0^2}\right), \tag{3}$$

где $\omega_c = \sqrt{\omega_0^2 - \alpha^2}$, $\alpha = \frac{1}{t_m}$, $\omega_0 = \frac{2\pi}{T_i}$.

Время t_m определяется положением максимума амплитуды сигнала на временной оси. Переменная составляющая в знаменателе отражает паразитную частотную модуляцию финитного сигнала.

Учитывая, что сформированный импульс побочного излучения за счет изменения токов в цепях ПК будет иметь короткую длительность ($t_в < \frac{2}{f_0}$), можно считать, что излученный сигнал будет не что иное, как реакция цепи на δ – функцию импульса тока, т.е. представляет собой импульсную характеристику цепи $g_ц(t)$, умноженную на площадь возбуждающего импульса $S_в$;

$$y(t) = \int_0^{\tau} x(\tau) g_ц(t-\tau) dt, \tag{4}$$

где $S_в = \int_0^{\tau_в} x(t) dt$.

Пространственно-временная импульсная характеристика цепи $g_ц(t_i, x, y, z)$ в режиме излучения представляет собой вектор напряженности электромагнитного поля в момент t_i в точке пространства с координатами (x,y,z) как реакция на входной импульс в пространство.

Импульсная характеристика антенны приёмника радиоперехвата побочных излучений ПК также представляет векторную функцию, компонентами которой являются соответствующие реакции на электромагнитное поле, полученные из точки пространства (x,y,z).

Для упрощения теоретического анализа спектра побочных излучений ПК сделаем допущения, не влияющие на общий результат:

- амплитуды импульсов каждого периода колебаний внутри интервала ($-\frac{mT}{2} \le t \le \frac{mT}{2}$) равны ($m$ – число периодов колебаний финитного сигнала);
- частота излучения постоянна ($f = \frac{1}{T} = const$).

Тогда спектр излученного сигнала в соответствии с преобразованием Фурье запишется в виде [4]:

$$\dot{S}(\omega) = \int_{-\frac{m\pi}{\omega_0}}^{\frac{m\pi}{\omega_0}} U_m \sin \omega_0 t e^{-j\omega t} dt = (-1)^{m_j} \frac{2U_m \omega_0 \sin(m\pi \omega / \omega_0)}{\omega_0^2 - \omega^2}, \qquad (5)$$

а модуль спектра определяется по формуле:

$$|S(f)| = \frac{U_m}{\pi f_0} \left| \frac{\sin(\pi m f / f_0)}{1 - (f / f_0)^2} \right|. \qquad (6)$$

Анализ выражения (6) показывает, что огибающая модуля спектра зависит от числа периодов колебаний финитного сигнала (m) и является несимметричной относительно несущей частоты (f_0), рис.3

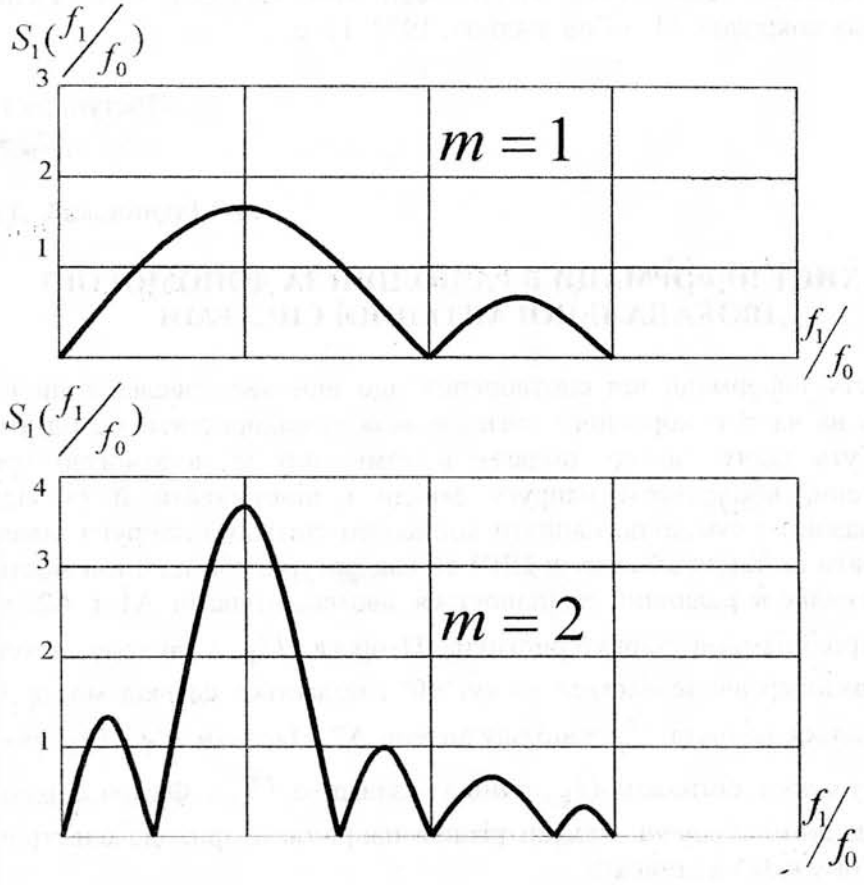

Рис.3 Спектр радиоимпульсов побочного излучения при $m = 1;2$.

Учитывая, что излучающие цепи ПК представляют собой полосовой фильтр (колебательный контур) с достаточно широкой полосой, следует ожидать, что количество периодов колебания будет не больше двух ($m \approx 1-2$), а в большинстве случаев только один.

Выводы.

1. Временная структура ПЭМИН в дальней зоне существенно отличается от информационных сигналов, циркулирующих в цепях ПК, но при определенных условиях позволяет путем несложных технических решений восстановить информационный сигнал.
2. Аналитическое представление временной структуры побочного излучения позволяет создать более эффективную имитирующую помеху средствам радиоперехвата при организации активной защиты компьютерной информации.

Список литературы:

1. Афинов В., В паутине МАСИНТа.,http:www.ng.ru/nvo.
2. Астанин Л.Ю., Костылев А.А., Сверхширокополосные радиолокационные измерители. М., «Воениздат»,1989, 127с.
3. Хармут Х.Ф. Теория секвентного анализа. Основы применения. М., «Мир», 1980, 458с.
4. Финкельштейн М.И., Мендельсон В.Л., Кутеев В.А. Радиолокация слоистых земных покровов. М., «Сов. Радио», 1977, 176с.

Поступила 14.01.2002

УДК 681.3.004

Л.Я.Ільницький, Л.В.Сібрук

ЗАХИСТ ІНФОРМАЦІЇ В РАДІОЛІНІЇ ЗА ДОПОМОГОЮ ДВОКАНАЛЬНОЇ АНТЕННОЇ СИСТЕМИ

Для захисту інформації від спотворення, що виникає внаслідок дії навмисних випромінювань на частоті корисного сигналу, можна використати метод амплітудної компенсації. Суть цього методу полягає в тому, що за допомогою просторової вибірності антени, виокремити напругу завади і підсумувати її (з відповідною амплітудою і фазою) з сумішшю напруги корисного сигналу і напруги завади. Метод можна реалізувати на таких елементах НВЧ як квадратурні або щілинні мости (рис. 1). Приймання сигналів в радіолінії здійснюється двома антенами А1 і А2, які мають однакові електродинамічні характеристики. Напруга $\dot{U}_1$ з виходу антени А1 в фіксованому фазообертачі зсувається на кут 90° і подається на вхід моста. На інший вхід моста подається напруга $\dot{U}_2$ з виходу антени А2. Напруги $\dot{U}_1$ і $\dot{U}_2$ мають по дві складові, одна з яких є сигналом $\dot{U}_k$, а інша – завадою $\dot{U}_{с.з}$. Фазові співвідношення між цими складовими створені завдяки різним напрямкам приходу електромагнітних хвиль (рис.2). Тому можна записати

$$\dot{U}_1 = l_\partial \dot{E}_k + l_\partial \dot{E}_{с.з} e^{i\psi} = \dot{U}_k + \dot{U}_{с.з} e^{i\psi}; \quad (1)$$

$$\dot{U}_2 = l_\partial \dot{E}_k + l_\partial \dot{E}_{с.з} e^{-i\psi} = \dot{U}_k + \dot{U}_{с.з} e^{-i\psi}, \quad (2)$$

де $\dot{E}_k$ і $\dot{E}_{с.з}$ - напруженості електричного поля корисного сигналу і сигналу завади; l_∂ - діюча довжина антен; $= 0.5kd\sin\theta$ - фазовий зсув, що виникає з причини різниці ходу променів; $k = 2\pi/\lambda$.