УДК 621.396

ИСПОЛЬЗОВАНИЕ МЕТОДА ВЧ-НАВЯЗЫВАНИЯ ДЛЯ ОРГАНИЗАЦИИ КАНАЛОВ УТЕЧКИ ЦИФРОВЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ СРЕДСТВАМИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

В.А. КОНДРАТЁНОК, О.В. ЧУРКО, А.М. БАКУРЕНКО

Военная академия Республики Беларусь

Поступила в редакцию 31 октября 2008

Рассмотрена проблема использования метода высокочастотного навязывания для организации каналов утечки цифровых данных, обрабатываемых средствами вычислительной техники, с использованием каналов передачи данных.

Ключевые слова: высокочастотное навязывание, канал утечки информации, канал передачи данных.

Введение

Технические каналы утечки информации, обрабатываемой средствами вычислительной техники (СВТ), возникающие за счет информационных наводок в сети их электропитания и заземления, представляют собой один из распространенных видов такого рода угроз безопасности информации [1]. Такого же мнения придерживаются авторы [2, 3] и др. Наряду с этим разработки [4] свидетельствуют о внимании заинтересованных лиц и организаций к обеспечению защиты СВТ от высокочастотного навязывания (ВЧ-навязывания).

Под "высокочастотным навязыванием", как показано в [5], понимается метод организации утечки информации, при котором в линию утечки подается высокочастотный сигнал от специального генератора. Этот сигнал за счет нелинейности элементов электронной аппаратуры взаимодействует с низкочастотными сигналами. Низкочастотный и высокочастотный сигналы, взаимодействуя, образуют сложную полиномную зависимость, приводящую к модуляции одного сигнала другим. При этом нелинейность электронных элементов аппаратуры играет роль модулятора низкими частотами высокочастотных колебаний, вводимых в аппаратуру через линию, а генератором является используемый "внешний" генератор высокой частоты.

Данный метод активно может применяться для организации утечки акустической информации [4–6], что же касается организации каналов утечки цифровых данных, обрабатываемых СВТ, открытая литература по этому вопросу отсутствует.

Авторы статьи считают целесообразным и необходимым проведение исследований по проблеме использования метода ВЧ-навязывания для разведки информации, обрабатываемой на СВТ, с использованием в том числе и каналов передачи данных (сетевых кабелей).

Формализация задачи анализа проблемы ВЧ-навязывания по сетевым кабелям

При рассмотрении проблемы ВЧ-навязывания по сетевым кабелям необходимо отметить следующие ее нюансы.

1. Элементом электронной аппаратуры, за счет нелинейности которого сигнал ВЧ-навязывания взаимодействует с низкочастотными (относительно него) сигналами, является элемент сетевого адаптера или модема.

Неизвестно при этом, какой элемент сетевого адаптера или модема считать "активным", т.е. элементом, свойства которого позволяют осуществить модуляцию высокочастотного сигнала и отражение его обратно в сеть.

По мнению авторов, в качестве "активного" следует рассматривать "выходной" нелинейный элемент (ВНЭ) сетевого адаптера или модема, к примеру транзистор (даже если его рассматривать в составе некоторой микросхемы, что часто и встречается). Влиянием последующих ("предвыходного" и т.д.) каскадов можно пренебречь, ввиду того что рабочий диапазон частот "выходного" нелинейного элемента обычно много ниже частоты сигнала ВЧ-навязывания, что обуславливает значительное его ослабление (на несколько порядков) при прохождении данного элемента.

2. Элементом электронной аппаратуры, который выполняет роль "модулятора", т.е. источником разведуемой информации, может быть видеокарта СВТ (является генератором в зависимости от типа видеокарты и монитора сигналов с частотой от 25 МГц до примерно 80 МГц [7]), любой внутренний (допускаем, что "утечек" через корпус нет) кабель (резонансные частоты внутренних кабелей могут находиться в диапазоне 200–800 МГц [7]) и т.д.

Следует при этом отметить, что частота сигнала ВЧ-навязывания должна быть, как минимум, в 10 раз выше частоты сигнала, который считается модулирующим (разведуемым). Это значит, что, разведывая сигнал видеокарты, у которого частота f_c=70 МГц, следует использовать сигнал ВЧ-навязывания с минимальной частотой $f_{ВЧ\text{-}н.}$=700 МГц и т.д. При этом весьма актуальным становится вопрос затухания такого сигнала и его "отражения" в сетевом кабеле.

Выходной нелинейный элемент и параметры сигнала ВЧ-навязывания

Как показывают результаты проведенного анализа имеющихся на рынке РБ сетевых адаптеров и модемов, "выходной" нелинейный элемент у них, как и предполагалось, входит в состав интегральной микросхемы, что не позволяет рассматривать его отдельно и анализировать характеристики данного элемента как выделенного. В составе сетевых адаптеров (модемов) "выходной" нелинейный элемент в ракурсе рассматриваемой проблемы выполняет следующие функции:

а) принимает сигнал ВЧ-навязывания;

б) изменяет свои характеристики под воздействием модулирующего (разведуемого) сигнала;

в) отражает обратно в линию сигнал (часть сигнала) ВЧ-навязывания, параметры которого изменяются в соответствии с изменениями параметров самого "выходного" нелинейного элемента;

г) рассеивает в виде тепла и пропускает в последующие каскады сетевого адаптера (модема) часть энергии сигнала ВЧ-навязывания.

При этом актуальными являются следующие вопросы:

1. Какую часть энергии сигнала ВЧ-навязывания можно позволить пропустить, не вызвав при этом сбоев в работе всего устройства (сетевого адаптера или модема) в целом? Данный аспект рассматриваемой проблемы важен, по мнению автором, в связи с тем, что одним из качеств мероприятий по разведке информации является их скрытность. Поэтому необходимо определить, какова может быть энергия высокочастотного сигнала (сигнала ВЧ-навязывания), прошедшего через "выходной" нелинейный элемент, при котором будут наблюдаться сбои функционирования устройства (сетевого адаптера или модема), а значит, можно будет определить факт попытки использования метода ВЧ-навязывания для организации каналов утечки цифровых данных, обрабатываемых СВТ, с использованием каналов передачи данных.

2. Какова должна быть доля рассеиваемой в виде энергии сигнала ВЧ-навязывания, которая сможет вызвать перегрев устройства и сбой его функционирования, а значит, и обнаружение факт попытки ВЧ-навязывания?

В свете перечисленного сигнал ВЧ-навязывания предлагается рассматривать не только как "зондирующий сигнал", но и как "помеху". Чем больше мощность сигнала ВЧ-навязывания, тем с большей дальности возможно проводить разведку, но при этом повышается вероятность сбоев функционирования "облучаемых" устройств, а значит, и вероятность вскрытия факта ведения разведки методом ВЧ-навязывания.

Изменение характеристик выходного нелинейного элемента под воздействием модулирующего (разведываемого) сигнала

Сопротивление нелинейного элемента в общем случае носит комплексный характер [8]. В процессе модуляции оно изменяется, а значит выходная проводимость данного элемента может быть охарактеризована в процессе модуляции переменными составляющими реактивной ($\Delta b_{\text{НЭ}}(t)$) и активной ($\Delta g_{\text{НЭ}}(t)$) проводимостей:

$$\Delta \dot{y}_{рл}(t) = \Delta g_{рл}(t) + j\Delta b_{рл}(t). \qquad (1)$$

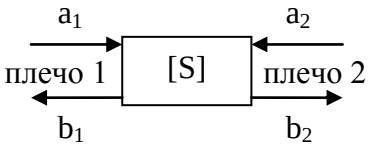
Под действием модулирующего напряжения будет изменяться как активная, так и реактивная составляющая проводимости нелинейного элемента. Изменение реактивной составляющей ($\Delta b_{\text{НЭ}}(t)$) будет вызывать частотную модуляцию, а активной составляющей ($\Delta g_{\text{НЭ}}(t)$) — амплитудную модуляцию.

Использование S-матрицы для описания процессов при ВЧ-навязывании

"Выходной" нелинейный элемент в составе интегральной микросхемы сетевого адаптера (модема) авторами статьи предлагается рассмотреть как некоторый четырехполюсник.

Как показано в [9], рассматриваемые существующие модели транзисторов могли бы применяться, если бы их элементы были изменены с высокой точностью. К сожалению, это не так. В связи с этим можно использовать бесструктурные модели, то есть представлять исследуемое устройство в виде некоторого "черного ящика", четырехполюсника, описываемого, к примеру, S-матрицей.

В настоящее время для описания многополюсников используются матрицы сопротивлений, проводимостей, отражения и рассеяния. В рассматриваемом случае использовать матрицу рассеяния [S] целесообразно. При этом, как показано на рисунке, анализируемый четырехполюсник имеет два плеча (*1* и *2*), входное и выходное.



S-матрица

Волна, выходящая из плеча *1*, имеет амплитуду b_1 и возбуждается волнами a_1 и a_2 на основе принципа суперпозиции:

$$\begin{cases} в_1 = s_{11}a_1 + s_{12}a_2 \\ в_2 = s_{21}a_1 + s_{22}a_2 \end{cases}, \qquad (2)$$

где $S_{\text{i,j}}$ — элементы S-матрицы;

$S = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix}$ — матрица рассеяния, устанавливающая связь отраженных от четырехполюсника (расходящихся от него) волн со сходящимися (падающими на него) волнами;

$S_{11} = \left.\dfrac{U_{1отр}}{U_{1пад}}\right|_{U_{2пад}=0}$ — комплексный коэффициент отражения от плеча *1* при согласованном плече *2*;

$S_{22} = \left.\dfrac{U_{2отр}}{U_{2пад}}\right|_{U_{1пад}=0}$ — комплексный коэффициент отражения от плеча *2* при согласованном плече *1*;

$S_{21} = \left.\frac{U_{2отр}}{U_{1пад}}\right|_{U_{2пад}=0}$ — комплексный коэффициент пропускания (передачи) из плеча *1* в плечо *2* при согласованном плече *2*;

$S_{12} = \left.\frac{U_{1отр}}{U_{2пад}}\right|_{U_{1пад}=0}$ — комплексный коэффициент пропускания (передачи) из плеча *2* в плечо *1* при согласованном плече *1*;

$$\begin{cases} U_{1отр} = S_{11}U_{1пад} + S_{12}U_{2пад} \\ U_{2отр} = S_{21}U_{1пад} + S_{22}U_{2пад} \end{cases}. \quad (3)$$

Рассмотренный случай соответствует исследованию электрической цепи с переменными во времени параметрами, к примеру нелинейного четырехполюсника, а в таких устройствах возможно возникновение следующих физический явлений [10].

Возникновение интенсивных колебаний в целом на высшей гармонике при отсутствии ее во входном напряжении.

Возникновение субгармонических колебаний, т.е. колебаний на частоте, в целое число раз меньше частоты источника ЭДС (чаще всего наблюдается колебания на частотах ω/2, ω/3, ω/5 и т.д.).

Возникновение колебаний в цепи на гармонике с частотой *m*ω/*n*, где *m, n* — целые числа.

Автомодуляция, хаотические колебания, перемежающиеся резонансы и другие явления.

Анализ данных физический явлений предполагается в ходе дальнейших исследований, результаты которых станут основой для последующей статьи.

Заключение

По результатам проведенных на данном этапе исследований в представленной статье авторами начата формализация решаемой задачи по анализу возможности организации утечки информации по каналам передачи данных при помощи ВЧ-навязывания, а именно выделены "выходной" и "модулирующий" элементы, предложена дуалистическая концепция предъявления требований к параметрам сигнала ВЧ-навязывания и как к "зондирующему сигналу", и как к "помехе".

Авторами не только намечены направления дальнейших исследований в рассматриваемой области, результаты которых планируется осветить в последующих публикациях, но и предложено использовать для описания процессов при ВЧ-навязывании с целью организации технических каналов утечки цифровой информации по каналам передачи данных аппарат S-матриц, что, предположительно, позволит существенно снизить временные затраты при моделировании данных процессов в связи с достаточно детальной проработкой упомянутого математического аппарата.

THE USING OF HIGH FREQUENCY DOMINATION METHOD FOR ORGANIZATION OF INFORMATION INTELLIGENCE TECHNICAL CHANNELS FOR DATA PROCESSING SYSTEMS

V.A. KONDRATYONOK, O.V. CHURCO, A.M. BAKURENKO

Abstract

The problem of using of high frequency domination method for organization of information intelligence technical channels for data processing systems is reflected.

Литература

1. *Пятачков А.Г.* // Защита информации. Конфидент. 2003. № 3. С. 82–87.
2. *Торокин А.А.* Инженерно-техническая защита информации. М., 2005.
3. *Куприянов А.И., Сахаров А.В., Шевцов В.А.* Основы защиты информации. М., 2006.
4. Комплекс оценки защищенности по каналу ВЧ-навязывания "ВЕПРЬ" / http://www.mascom.ru/article614.asp.htm.
5. *Халяпин Д.Б.* Защита информации. Вас подслушивают? Защищайтесь. М., 2004.
6. *Бузов Г.А., Калинин С.В., Кондратьев А.В.* Защита от утечки информации по техническим каналам. М., 2005.
7. *Хореев А.А.* // Защита информации. Inside. 2008. № 1. С. 28–36.
8. *Павловский А.В., Макаров И.В., Шаров Д.А.* Радиопередающие устройства. Ч. 1 и Ч. 2 Минск, 2006.
9. *Шварц Н.З.* Линейные транзисторные усилители СВЧ. М., 1980.
10. *Бессонов Л.А.* Теоретические основы электротехники. Электрические цепи. М., 1996.