ОСОБЕННОСТИ СИСТЕМ КОНТРОЛЯ ИНФОРМАЦИОННЫХ ПОТОКОВ БОЛЬШОГО РАЗМЕРА

Для построения комплексных систем защиты информации и других систем безопасности необходим анализ рисков. При обслуживании систем передачи данных большого размера в оптических линиях связи наблюдение за информацией является сложной задачей. Оно требует применения новых аппаратных решений в средствах контроля и сбора данных, которые являются исходной информационной базой будущих проектов. Рассмотрена проблема использования средств защиты информации при проектировании комплексных систем защиты информации. Главное внимание уделяется методам контроля за потоками информации більшого размера, которые доступны атакам киберпреступников. Рассматриваются вопросы применяемых на рынках Украины и за ее пределами таких систем контроля, функциональные возможности которых позволяют решать задачи защиты от кибертерроризма при их использовании в качестве средств защиты информации в рамках проектов комплексних систем защиты.

Ключевые слова: комплексная система защиты информации; проект защиты; линии связи; сетевой экран; сетевой комплект.

FEATURES OF MONITORING SYSTEMS OF INFORMATION SIZABLE STREAMS

The analysis is necessary for construction of complex systems of protection of the information and other systems of safety to risk. At service of systems of sizable data transmission in optical communication lines supervision over the information is a complicated problem. It demands application of new hardware decisions in means of the control and data gathering which are initial information base of the future projects. The problem of use of new means of protection of the information is considered at designing complex systems of protection of the information. The main attention is given a quality monitoring for streams of the information of the big size, and which are accessible to attacks Cybernetic criminals. Questions used on the markets of Ukraine and behind its limits of such monitoring systems which functionalities allow to solve tasks of protection from Cybernetic terrorism at their use as means of protection of the information within the framework of projects systems of complex of protection are considered.

Index Terms: System of Complex of Protection of the Information; the project of protection; communication lines, the network screen; the network complete set.

Луценко Владимир Николаевич, кандидат технических наук, старший научный сотрудник Академии наук Украины, доцент Физико-технического института НТУУ «КПИ».
E-mail: lutsenkovn@ukr.net
Луценко Володимир Миколайович, кандидат технічних наук, старший науковий співробітник Академії наук України, доцент Фізико-технічного інституту НТУУ «КПІ».
Lutsenko Vladimir, Ph.D., Senior Research Fellow of the Academy of Sciences of Ukraine, Assistant Professor of Physics and Technical Institute of NTU «KPI2.

Балан Андрей Николаевич, аспирант очного отделения Физико-технического института, НТУУ «КПИ».
E-mail: ftzzi@pti.kpi.ua
Балан Андрій Миколайович, аспірант Фізико-технічного інституту, НТУУ «КПІ».
Balan Andrej, the post-graduate student of physicotechnical institute of the «KPI».

УДК 621.372

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СВЧ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ПО ЦЕПИ ЭЛЕКТРОПИТАНИЯ

Валерий Козловский, Роман Лысенко

Для построения фильтрующих устройств СВЧ (сверх высоких частот) с целью предотвращения утечки информации по цепям электропитания необходимо учитывать влияние внешних экранов. Существующие методы синтеза устройств фильтрации основаны на использовании математической модели двухпроводной линии передачи без учёта эффекта экранирования внешней оболочкой. В результате аплитудно-частотная характеристика фильтра отличается от экспериментальной, что приводит к ухудшению фильтрации в полосе заграждения. Предложено использовать в качестве концептуальной математической модели элемента фильтра модель связанной линии передачи. Концептуальная модель позволяет учитывать эффект экранирования внешней оболочки и повышает точность расчета устройств фильтрации цепей электропитания.

Ключевые слова: *связанная линия, восьмиполюсник, четырехполюсник, чётное и нечётное возбуждение, волновое сопротивление.*

Введение. Как известно [1], цепи электропитания являются одним из основных электрических каналов утечки информации различных телекоммуникационных систем, а также средств вычислительной техники (СВТ), предназначенных для обработки информации ограниченного доступа. Появление информационных сигналов в цепи электропитания СВТ возможно как за счет наводок побочных электромагнитных излучений (ПЭМИ), так и за счет внутренних паразитных ёмкостных и (или) индуктивных связей выпрямительного устройства блока питания СВТ [1, 2].

Одним из методов предотвращения утечки информации является фильтрация [1]. Фильтрация опасных сигналов осуществляется с целью предотвращения распространения высокочастотных информационных сигналов за пределы контролируемой зоны (КЗ). Для фильтрации сигналов в цепях питания в настоящее время используются помехоподавляющие фильтры [1]. В настоящее время существует большое количество различных типов помехоподавляющих фильтров, обеспечивающих ослабление нежелательных сигналов в разных участках частотного диапазона. Для исключения проникновения информационных сигналов в цепи электропитания используются фильтры нижних частот (ФНЧ) [1, 2], которые пропускают сигналы с частотами ниже граничной частоты ($f \le f_{гр}$) и подавляют - с частотами выше граничной частоты. Последовательная ветвь ФНЧ должна иметь малое сопротивление для постоянного тока и нижних частот. Вместе с тем, для того чтобы высшие частоты задерживались фильтром, последовательное сопротивление должно расти с частотой. Этим требованиям удовлетворяет индуктивность. Параллельная ветвь ФНЧ, наоборот, должна иметь малую проводимость для низких частот с тем, чтобы токи этих частот не шунтировались параллельным плечом. Для высоких частот необходимо, чтобы параллельная ветвь обладала большей проводимостью, тогда колебания этих частот будут ею шунтироваться, и их ток на выходе фильтра – ослабляться. Таким требованиям отвечает емкость. Более сложные многозвенные ФНЧ (Чебышева, Баттерворта, Бесселя и т. д.) конструируют на основе сочетаний различных единичных звеньев.

Существующие методы построения помехоподавляющих фильтров позволяют предотвратить утечку информации приблизительно до частот 1 ГГц. В этом диапазоне частот используются как сосредоточенные фильтры, так и фильтры комбинированного типа, использующие сосредоточенные и полураспределённые элементы. На частотах свыше 1 ГГц используются распределённые фильтры (полосковые, коаксиальные или волноводные).

При построении фильтров с распределёнными параметрами в связанных структурах электропитания возникает проблема подавления нерабочих пространственных полей, которые образуют искусственные (фантомные) каналы утечки информации. Существование фантомных каналов обусловлено сложной пространственной структурой электромагнитного поля в области пространства цепи питания. Существующие методы синтеза фильтров [2, 3] учитывают только один тип колебаний (одну пространственную структуру поля). Поэтому распределённый фильтр, рассчитанный на подавление сигналов одного типа колебаний, может вообще не фильтровать сигналы тех же самых частот, но имеющих другую структуру поля. Именно эти высшие типы колебаний и образуют дополнительные (фантомные) каналы утечки информации, которые в настоящее время не учитываются при построении фильтров в цепях питания.

Целью статьи является разработка концептуальной (содержательной) модели цепи питания с учётом фантомного канала.

Основная часть. Рассмотрим сечения наиболее распространённых цепей питания, показанные на рис. 1.

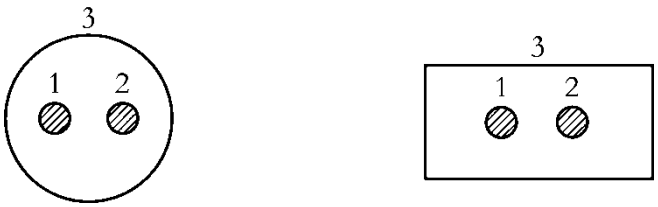

Рис. 1. Двухпроводные экранированные линии питания: 1,2 – проводники для подачи питания; 3 – экран

При передаче информации в диапазоне СВЧ проводники цепи питания при условии, что поперечный размер сечения значительно меньше длины волны, образуют линию передачи. Из-за наличия заземляющего экрана цепи питания (рис. 1) образует систему двух связанных линий. В такой системе распространение волн возможно по двум путям: между проводами, когда ток проходит по одному проводу и возвращается по другому (рис. 2, *a*), и по пути два провода – экран, когда ток проходит по двум проводам в одном направлении и возвращается через экран (рис. 2, *b*).

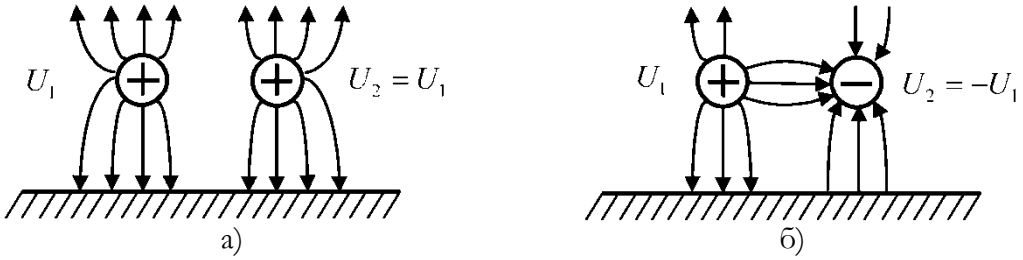

Рис. 2. Структура электрического поля при возбуждении двух связанных линий:
а) - чётное (синфазное) возбуждение; б) - нечётное (противофазное) возбуждение

Каждый из этих путей можно рассматривать как отдельный волновой канал, который характеризуется своими волновыми параметрами. Электрические сигналы в общем случае распространяются по обоим волновым каналам в виде двух независимых волн.

Каждый из каналов представляет собой линию передачи со своим волновым сопротивлением.

Рассмотрим эти линии передачи в режиме бегущих волн, то есть когда каждая линия нагружена на соответствующее волновое сопротивление.

В общем случае электромагнитное поле в сечении цепи питания из-за несовершенства экранировки отдельных узлов и устройств аппаратуры имеет сложную структуру. Поэтому на входе связанной линии одновременно возникают две волны (моды) напряжения и тока, соответствующие чётному и нечётному возбуждению (рис. 2). На однородных участках линии обе волны распространяются независимо одна от другой, то есть накладываются друг на друга, не взаимодействуя.

Предположим, что проводники 1 и 2 (рис. 1, 2) относительно экрана имеют напряжение U_1, U_2. Определим чётную и нечётную моду в каждом проводнике. Для этого учтём тот факт, что напряжение в каждом проводнике является суммой чётного и нечётного напряжения в данном проводнике. То есть

$$U_1 = U_{1ч} + U_{1н},\ U_2 = U_{2ч} + U_{2н}. \quad (1)$$

Далее учтём, что рассматриваемые линии являются симметричными (рис.1, 2). Тогда в соответствии с рис. 2 имеем

$$U_2 = U_{2ч} + U_{2н} = U_{1ч} - U_{1н}. \quad (2)$$

Воспользовавшись выражениями (1, 2), находим чётную и нечётную моду:

$$U_{1ч} = 0{,}5(U_1 + U_2),\ U_{1н} = 0{,}5(U_1 - U_2). \quad (3)$$

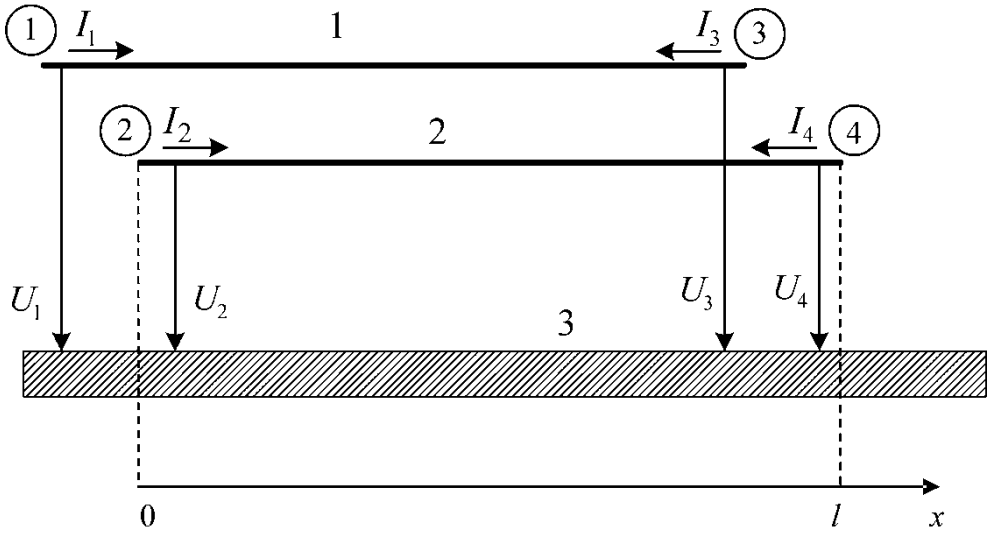

Рис. 3. Распределённый восьмиполюсник на связанных линиях

Формулы (1-3) позволяют по заданному возбуждению определить чётную и нечётную моды и, наоборот, по известным модам определить напряжения возбуждения.

В тех случаях, когда нагрузки связанных линий не равны волновым сопротивлениям мод или когда имеются нерегулярности в линии питания, то следует учитывать взаимное преобразование мод. В этом случае цепи питания (рис. 1, 2)

следует рассматривать как распределённый восьмиполюсник, составленный из двух связанных линий (рис. 3). При этом связанные проводники 1, 2 (рис. 3) соответствуют проводникам 1, 2 линий питания (рис. 1), а экран 3 (рис. 1) соответствует земляному проводу 3 связанных линий (рис. 3). Схема рис. 3 будет справедлива также и в случае, когда линия питания несимметрична, например, в случае различных сечений проводников 1, 2 (рис. 1).

Если связанные линии однородны по длине (регулярны) то матрица сопротивлений эквивалентного восьмиполюсника имеет следующий вид [3]:

$$Z=\begin{bmatrix} Z_{11} & Z_{12} & Z_{13} & Z_{14} \\ Z_{21} & Z_{22} & Z_{23} & Z_{24} \\ Z_{31} & Z_{32} & Z_{33} & Z_{34} \\ Z_{41} & Z_{42} & Z_{43} & Z_{44} \end{bmatrix}, \quad \begin{aligned} Z_{11}&=Z_{22}=Z_{33}=Z_{44}=-0{,}5\,j(Z_{oe}+Z_{oo})ctg\,\theta, \\ Z_{12}&=Z_{21}=Z_{43}=Z_{34}=-0{,}5\,j(Z_{oe}-Z_{oo})ctg\,\theta, \\ Z_{13}&=Z_{31}=Z_{24}=Z_{42}=-0{,}5\,j(Z_{oe}+Z_{oe})\cos ec\,\theta, \\ Z_{14}&=Z_{41}=Z_{32}=Z_{23}=-0{,}5\,j(Z_{oe}-Z_{oo})\cos ec\,\theta, \end{aligned} \tag{4}$$

где $Z_{\text{ое}}, Z_{oo}$ - волновые сопротивления, соответствующие чётному и нечётному напряжению в линии; θ – электрическая длина линии, $\theta=\omega l/v_\phi$, l – длина линии (рис.3), v_ϕ – фазовая скорость распространения волны в линии.

Аналогично записывается и матрица проводимостей. В этом случае в формулах (4) следует заменить волновые сопротивления на волновые проводимости.

В тех случаях, когда связанная линия состоит из набора линий с различными чётными и нечётными волновыми сопротивлениями (например при включении фильтра нижних частот), удобно пользоваться A - матрицами. На основании (4) A - матрица отрезка одинаковых связанных линий записывается следующим образом

$$\mathbf{A}=\begin{bmatrix} \cos\theta & 0 & j0{,}5(Z_{\text{ое}}+Z_{oo})\sin\theta & j0{,}5(Z_{\text{ое}}-Z_{oo})\sin\theta \\ 0 & \cos\theta & j0{,}5(Z_{\text{ое}}-Z_{oo})\sin\theta & j0{,}5(Z_{\text{ое}}+Z_{oo})\sin\theta \\ j\dfrac{0{,}5(Z_{\text{ое}}+Z_{oo})}{Z_{\text{ое}}Z_{oo}}\sin\theta & -j\dfrac{0{,}5(Z_{\text{ое}}-Z_{oo})}{Z_{\text{ое}}Z_{oo}}\sin\theta & \cos\theta & 0 \\ -j\dfrac{0{,}5(Z_{\text{ое}}-Z_{oo})}{Z_{\text{ое}}Z_{oo}}\sin\theta & j\dfrac{0{,}5(Z_{\text{ое}}+Z_{oo})}{Z_{\text{ое}}Z_{oo}}\sin\theta & 0 & \cos\theta \end{bmatrix}. \tag{5}$$

Таким образом, A - матрица многоступенчатой связанной линии будет равна произведению A - матриц типа (4).

В общем случае в распределённой линии питания могут присутствовать сосредоточенные или распределённые включения, например за счёт несанкционированного подключения. Поэтому представляет интерес определение параметров восьмиполюсника, составленного из двух несвязанных четырёхполюсников, каждый из которых характеризует дополнительное подключение.

Рассмотрим два четырёхполюсника (рис. 4) имеющих A-матрицы $A^{(1)}, A^{(2)}$. В системе A – параметров связь между токами и напряжениями в восьмиполюснике записывается в виде [3]

$$\left.\begin{aligned} U_1&=A_{11}U_3+A_{12}U_4+A_{13}I_3+A_{14}I_4 \\ U_2&=A_{21}U_3+A_{22}U_4+A_{23}I_3+A_{24}I_4 \\ I_1&=A_{31}U_3+A_{32}U_4+A_{33}I_3+A_{34}I_4 \\ I_2&=A_{41}U_3+A_{42}U_4+A_{43}I_3+A_{44}I_4 \end{aligned}\right\}. \tag{6}$$

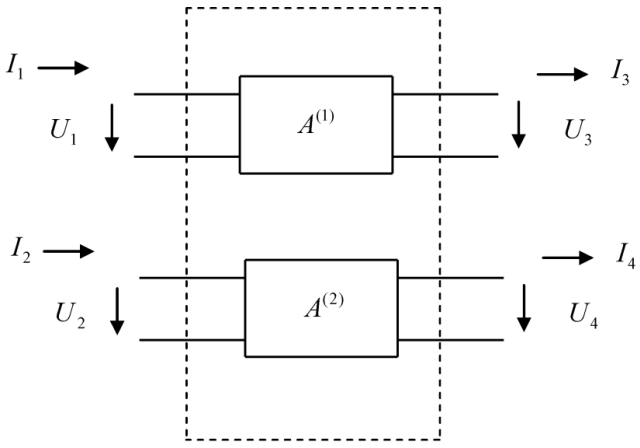

Рис. 4. Восьмиполюсник, состоящий из двух несвязанных четырёхполюсников

Перепишем данные уравнения (6) в матричной форме

$$\begin{bmatrix} U_1 \\ U_2 \\ I_1 \\ I_1 \end{bmatrix}=\mathbf{A}\begin{bmatrix} U_3 \\ U_4 \\ I_3 \\ I_4 \end{bmatrix},\ \mathbf{A}=\begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} \\ A_{21} & A_{22} & A_{23} & A_{24} \\ A_{31} & A_{32} & A_{33} & A_{34} \\ A_{41} & A_{42} & A_{43} & A_{44} \end{bmatrix}. \tag{7}$$

С другой стороны для каждого из четырёхполюсников (рис. 4) справедливы уравнения

$$\begin{bmatrix} U_1 \\ I_1 \end{bmatrix} = \begin{bmatrix} A_{11}^{(1)} & A_{12}^{(1)} \\ A_{21}^{(1)} & A_{22}^{(1)} \end{bmatrix} \cdot \begin{bmatrix} U_3 \\ I_3 \end{bmatrix}, \quad \begin{bmatrix} U_2 \\ I_2 \end{bmatrix} = \begin{bmatrix} A_{11}^{(2)} & A_{12}^{(2)} \\ A_{21}^{(2)} & A_{22}^{(2)} \end{bmatrix} \cdot \begin{bmatrix} U_4 \\ I_4 \end{bmatrix}. \quad (8)$$

Сопоставляя уравнения (6, 7) с (8), находим уравнение восьмиполюсника рис. 4:

$$\begin{bmatrix} U_1 \\ U_2 \\ I_1 \\ I_1 \end{bmatrix} = \mathbf{A} \begin{bmatrix} U_3 \\ U_4 \\ I_3 \\ I_4 \end{bmatrix}, \ \mathbf{A} = \begin{bmatrix} A_{11}^{(1)} & 0 & A_{12}^{(1)} & 0 \\ 0 & A_{11}^{(2)} & 0 & A_{12}^{(2)} \\ A_{21}^{(1)} & 0 & A_{22}^{(1)} & 0 \\ 0 & A_{21}^{(2)} & 0 & A_{22}^{(2)} \end{bmatrix}. \quad (9)$$

Воспользуемся полученными результатами для определения матрицы восьмиполюсника, состоящего из последовательного комплексного сопротивления Z (рис. 5).

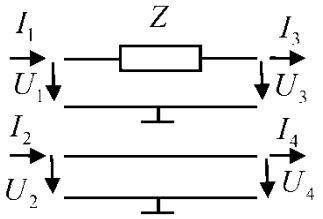

Рис. 5. Последовательно включённое сопротивление

В данном случае матрицы независимых четырёхполюсников соответственно равны

$$\mathbf{A^{(1)}} = \begin{bmatrix} 1 & Z \\ 0 & 1 \end{bmatrix}, \ \mathbf{A^{(2)}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \quad (10)$$

Тогда, согласно (9), имеем матрицу восьмиполюсника рис. 5

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & Z & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (11)$$

Заключение. Изложенные выше результаты представляют концептуальную модель канала утечки информации по цепи питания, реализованной в виде двухпроводной экранированной линии и её различных модификаций: двухпроводная линия в прямоугольном экране, различные варианты связанных полосковых линий [4].

С помощью полученных соотношений появляется возможность анализа различных цепей питания в СВЧ диапазоне с сосредоточенными и распределёнными включениями.

Из вышеизложенного следует, что при построении фильтров цепей питания обязательно следует учитывать распространение двух волн: чётной и нечётной, для которых волновые сопротивления линий различны. При этом нерабочий тип колебания образует искусственный канал утечки информации.

ЛИТЕРАТУРА

[1]. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. - К.: Юниор, 2003. – 502 с.

[2]. Максимов Ю. Н., Сонников В. Г., Петров В. Г. Технические методы и средства защиты информации. - СПб.: ООО «Издательство Полигон», 2000. - 320 с.

[3]. Thomas H. Lee. Planar Microwave Engineering: A Practical Guide to Theory, Measurement, and Circuits. Cambridge University Press, 2004.- 862 p.

[4]. Ганстон М.А.П. Справочник по волновым сопротивлениям фидерных линий СВЧ.-М.: Связь, 1976.- 152 с.

REFERENCES

[1]. Khoroshko V.A., Chekatkov A.A. Methods and tools for information security., K.: Junior, 2003., 502 p.

[2]. Maksimov Y.N., Sonnikov V.G., Petrov V.G. Technical methods and tools of information protection., St. Petersburg. LLC "Publishing Polygon", 2000., 320 p.

[3]. Thomas H. Lee. Planar Microwave Engineering: A Practical Guide to Theory, Measurement, and Circuits. Cambridge University Press, 2004., 862 p.

[4]. Ganstan I.A.O. Reference book Characteristic impedance of microwave feeder.-M.: Communication, 1976., 152 p.

КОНЦЕПТУАЛЬНА МОДЕЛЬ НВЧ КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ В КОЛІ ЕЛЕКТРОЖИВЛЕННЯ

Для побудови фільтруючих пристроїв НВЧ (над високих частот) з метою запобігання витоку інформації по колах електроживлення необхідно враховувати вплив зовнішніх екранів. Існуючі методи синтезу пристроїв фільтрації засновані на використанні математичної моделі двопровідної лінії передачі без урахування ефекту екранування зовнішньою оболонкою. В результаті аплітудно-частотна характеристика фільтра відрізняється від експериментальної, що призводить до погіршення фільтрації в смузі загородження. Запропоновано використовувати в якості концептуальної математичної моделі елемента фільтра модель пов'язаної лінії передачі. Концептуальна модель дозволяє враховувати ефект екранування зовнішньої оболонки і підвищує точність розрахунку пристроїв фільтрації в колах електроживлення.

Ключові слова: пов'язана лінія, восьмиполюсник, чотириполюсник, парне і непарне збудження, хвильовий опір.

A CONCEPTUAL MODEL OF THE MICROWAVE CHANNEL OF INFORMATION LEAKAGE BY THE POWER SUPPLY CIRCUIT

For the construction of the microwave filter devices to prevent information leakage on the supply lines should take into account the impact of external screens. Existing methods for the synthesis filtering devices are based on the mathematical model the two-wire transmission line, excluding the effect of shielding the outer envelope. As a result, the frequency response function of the filter is different from the experimental, which leads to deterioration in the band rejection filter. Proposed as a conceptual mathematical model of the filter element model coupled transmission line. The conceptual model takes into account the effect of shielding the outer shell and increases the accuracy of calculating the filtration devices in the power supply circuit.

Index Terms: coupled transmission line, eight-pole network, four-pole network, even and odd excitation, wave impedance.

Козловский Валерий Валерьевич, кандидат технических наук, доцент Государственного университета информационно-коммуникационных технологий.
E-mail: valerey@ukr.net

Козловський Валерій Валерійович, кандидат технічних наук, доцент Державного університету інформаційно-комунікаційних технологій.
Kozlowskiy Valeriy, Ph.D. in Eng., associate professor of the State University of Information and Communication Technologies.

Лысенко Роман Михайлович, аспирант Института специальной связи и защиты информации Национального технического университета Украины «КПИ», главный научный сотрудник Государственной службы специальной связи и защиты информации Украины.
E-mail: romanukr@list.ru

Лисенко Роман Михайлович, аспірант Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «КПІ», головний науковий співробітник Державної служби спеціального зв'язку та захисту інформації України.
Lysenko Roman, PhD student of Institute of Special Communication and Information Security of National Technical University of Ukraine «KPI», Chief Scientific Officer of the State Service of Special Communication and Information Protection of Ukraine.

УДК 004.056.53(045)

СИСТЕМА ФОРМИРОВАНИЯ НЕЧЕТКИХ ЭТАЛОНОВ СЕТЕВЫХ ПАРАМЕТРОВ

Анна Корченко

На основе известного метода выявления аномалий порожденных кибератаками разработана соответствующая система, для поддержки функционирования которой необходима реализация средства формирования нечетких эталонов, ориентированного на измерение текущих значений параметров сетевого трафика с целью выявления подозрительной активности в среде окружения. Для решения такой задачи предложено новое структурное решение соответствующей системы, состоящей из регистра эталонов, атак и параметров, а также блоков коммутации параметров, связывания атаки с параметром, формирования совокупности термов, формирования эталонов, регистра эталонов и процессора визуализации эталонов. Эта разработка может быть реализована программно или программно-аппаратно и ориентирована на измерение текущих значений параметров сетевого трафика с целью идентификации аномального состояния.

Ключевые слова: *кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях, нечеткие эталоны.*

Использование методов и моделей нечетких множеств для построения средств обнаружения аномалий, порожденных атакующими действиями, позволит усовершенствовать существующие системы выявления вторжений и, путем контроля активности в среде окружения, идентифицировать опасные аномальные состояния. Для этого в работах [1-2] разработана базовая модель параметров и универсальная модель эталонов лингвистических переменных (ЛП), которые за счет сформированных множеств пар, связывающих тип атаки с параметрами и набором логико-лингвистических связок, позволяют формализовать процесс построения эталонных значений для заданной среды окружения, отображать и устанавливать соответствие между типом атаки и необходимыми для ее идентификации атрибутами, а также измерять аномальное