Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

ПРИЛОЖЕНИЕ СИГНАЛЬНЫХ ГРАФОВ И МАТРИЧНОГО АНАЛИЗА ДЛЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

Д.С. РЯБЕНКО, В.К. ЖЕЛЕЗНЯК, С.В. ЛАВРОВ, С.Н. АБРАМЕНКО

Полоцкий государственный университет

Высокая степень интеграции микроэлектроники, стремительное развитие технологических и информационных процессов обусловили новые принципиальные решения защиты информации от утечки. Методическая и вычислительная оптимизация новых решений направлена на устранение противоречий между схемными и конструктивными параметрами и их защищенностью. Главная проблемная научно-практическая задача направлена на исключение паразитных информационных связей, благодаря минимизации, высокой плотности компоновки бескорпусных активных элементов, применению больших и сверхбольших интегральных схем [1]. Технология монтажа многослойных печатных плат ограничивает доступ к измерению и контролю параметров и характеристик схем. Паразитные связи благодаря взаимным наводкам снижают быстродействие управлением и обменом информацией. Вторая проблема – защита радиоэлектронных средств различного назначения от радиопомех [2].

Физические и математические модели устанавливают рациональные методы исследования сложных информационных систем на всех стадиях их жизненного цикла и их элементов (блоки, печатные платы). Показатели защищенности оценивают в условиях активной и пассивной защиты каждого канала утечки информации.

Точностные и временные параметры оценивают на соответствие критериев (показателей) защищенности каналов утечки информации [3, 4].

Проанализирована схемно-конструктивная оценка защищенности информации с использованием направленных графов и корреляционных функций электронных устройств. Исследование сложных многоконтурных и многосвязных систем с использованием их топологических свойств элементов матриц, отличающиеся значительным объемом обрабатываемой информации со сложными связями как между объектами, связывающими информационные системы, объектами информатизации, так и элементы более низкого уровня, т.е. структурные схемы или графы.

Структурные схемы, как и графы для многосвязных систем большой размерности становятся чрезвычайно сложными для исследований.

Причинно-следственные связи между значениями токов и напряжений, схемными решениями исследуют и используют теорию сигнальных графов, матричной алгебры, матричного преобразования, расчета их входных и выходных параметров, матричного преобразования h-параметров транзистора [5]. Качество и достоверность оценки сигналов при обработке в матричной форме весьма актуальна.

Сигнальные графы содержат ребра и вершины (узлы) исследований токов (напряжений) с определенным направлением (ориентированный граф). Ориентированный граф $G = (V, E)$, где V – множество вершин, E – множество ребер, анализируется с помощью матрицы смежности и матрицы инциденций [6].

Специальные векторные и матричные структуры обеспечивают матричные операции, матрицы представляют емкий метод систематизации алгебраических и численных соотношений [7].

Матрица инциденций A с n строками, соответствующими вершинам, и m столбцам, соответствующим ребрам. Для ориентированного графа столбец, соответствующий дуге $\langle x, y\rangle \in E$, содержит -1 в строке, соответствующей вершине x, 1 в строке, соответствующей вершине y, и нули во всех остальных строках. Петлю, т.е. дугу в виде $\langle x, x\rangle$ удобно представлять значением в строке x, например 2 [6, 7].

Матричное уравнение Ax = 0. Матрицу А представили в виде суммы двух матриц [8]

$$\text{А} = \text{Д} + \text{С}, \tag{1}$$

где $\text{А} = \begin{bmatrix} n \\ a_{ij} \\ i, j = 1 \end{bmatrix}$, $\text{Д} = \begin{bmatrix} n \\ a_{ii} \\ i = 1 \end{bmatrix}$, $\text{С} = \begin{bmatrix} n \\ a_{ij} \\ i \neq j \end{bmatrix}$.

Уравнение (1) в развернутой форме

$$\text{А} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} = \begin{bmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & a_{22} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_{nn} \end{bmatrix} + \begin{bmatrix} 0 & a_{12} & \ldots & a_{1n} \\ a_{21} & 0 & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & 0 \end{bmatrix}. \tag{2}$$

Из (2) следует, что матрица Д состоит только из диагональных членов, матрица С – только из недиагональных. Матрица А получена из системы алгебраических уравнений и представлена линейным однородным уравнением в матричной форме (1). Развернутая форма уравнения (2) с относительно главным членом, слагаемым с одинаковыми цифрами в индексе (a_{11}, a_{22}, …a_{nn}).

Элементы матрицы Д являются собственными операторами системы, а элементы матрицы С – операторами связей [8].

Транспонированная матрица А получена заменой строк матрицы А соответственно столбцами матрицы А^{T} и е столбцов – строками матрицы А [9]

$$\text{А}^{\text{T}} = \begin{bmatrix} a_{11} & a_{21} & \ldots & a_{n1} \\ a_{12} & a_{22} & \ldots & a_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{nn} \end{bmatrix}. \tag{3}$$

Разделяют все элементы матрицы (3) на величину определителя.

Определитель (детерминант) вырожденной квадратной nxn-матрицы определяется выражением [7]

$$\det A = \sum_{j=1}^{n} (-1)^{1+j} a[1, j] A_{1j}, \tag{4}$$

где $a[1, j]$ – элемент из верхней строки матрицы А, а A_{1j} – определитель (n-1)x(n-1)-матрицы, образованной отбрасыванием первой строки и j-го столбца nxn-матрицы А. Квадратная nxn-матрица вырожденная тогда и только тогда, когда detA = 0. Если detA ≠ 0, то матрица А обратима. Определитель произведения двух квадратных nxn-матриц А и В равен произведению определителей этих матриц $\det \text{AB} = \det \text{A} \cdot \det \text{B}$.

Единичная матрица Е, произведенная из матрицы А и обратной ей матрицы A^{-1}, полученной из обращения матрицы А и умноженной как справа, так и слева на матрицу А [10].

$AA^{-1} = A^{-1}A = E$, где Е – единичная матрица, A^{-1} – обратная неособенная квадратная матрица матрице А. Неособенная матрица *n*-го порядка [10]

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, \text{ где } \det A = \Delta \neq 0.$$

Для матрицы А присоединительная матрица $\tilde{A}$

$$\tilde{A} = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{bmatrix},$$

где A_{ij} – алгебраические дополнения (миноры со знаками) соответствующих элементов a_{ij} ($i, j = 1, 2, \dots n$).

Разделив все элементы матрицы $\tilde{A}$ на величину определителя Δ матрицы А:

$$A^* = \begin{bmatrix} A_{11}/\Delta & A_{21}/\Delta & \dots & A_{n1}/\Delta \\ A_{12}/\Delta & A_{22}/\Delta & \dots & A_{n2}/\Delta \\ \dots & \dots & \dots & \dots \\ A_{1n}/\Delta & A_{2n}/\Delta & \dots & A_{nn}/\Delta \end{bmatrix}.$$

Произведение AA^* позволяет получить [10]

$$AA^* = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} A_{11}/\Delta & A_{21}/\Delta & \dots & A_{n1}/\Delta \\ A_{12}/\Delta & A_{22}/\Delta & \dots & A_{n2}/\Delta \\ \dots & \dots & \dots & \dots \\ A_{1n}/\Delta & A_{2n}/\Delta & \dots & A_{nn}/\Delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix} = E. \qquad (5)$$

Из матрицы (2) получены две диагональные матрицы Д и С, по которым можно оценить уровень излучения (тока), а также уровень связей.

Список литературы

1. Мигулин И.Н. Интегральные микросхемы в радиоэлектронных устройствах. – К.: Техника, 1985. 208 с.

2. Тихонов В.И., Харисов В.Н. Статистический анализ и синтез радиотехнических устройств и систем: уч. пособие для вузов. – М.: Радио и связь, 1991. 608 с.

3. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие. СПб.: ГУАП, 2006. 188 с.

4. Кошевая Л.А. Обеспечение единства испытаний. Концептуальные основы. – К.: НАУ-друк, 2009. 176 с.

5. Расчет транзисторных цепей / под ред. Р.Ф. Ши. – М.: Энергия, 1964. 204 с.

6. Корни Ш. Теория цепей. Анализ и синтез. М.: Связь, 1973. 308 с.

7. Марпл-мл. С.Л. Цифровой спектральный анализ и его приложения. – М.: Мир, 1990. 584 с.

8. Шатихин Л.Г. Структурные матрицы и их применение для исследования систем. – М.: Машиностроение, 1974. 248 с.

9. Липницкий В.А. Высшая математика. Основы линейной алгебры и аналитической геометрии : уч. пособие для курсантов учреждений высшего образования. – Минск: ВА РБ. 2015. 229 с.

10. Демидович Б.П., Марон П.А. Основы вычислительной математики : учеб. пособие для студ. высш. техн. учеб. заведений. – М.: Наука, 1970. 664 с.

АНАЛИЗ ЭФФЕКТИВНОСТИ И ПОМЕХОЗАЩИЩЕННОСТИ МНОГОКАНАЛЬНЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ С КОДОВЫМ УПЛОТНЕНИЕМ

В.О. СИДОРОВИЧ, А.Н. ГАВРИЧЕНКО, А.Е. ВАРЮШИНА

Научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации»

Введение

Практика построения современных СПИ показывает, что наиболее дорогостоящими звеньями трактов передачи являются линии связи (кабельные, волоконно-оптические, сотовой мобильной радиосвязи, радиорелейной и спутниковой связи и т. д.). Поскольку экономически нецелесообразно использовать дорогостоящую линию связи для передачи информации единственной паре абонентов, то возникает необходимость построения многоканальных СПИ, обеспечивающих передачу большого числа сообщений различных источников информации по общей линии связи [1].

В многоканальной СПИ по общему высоко-частотному тракту передаются сообщения от нескольких источников информации. На передающей стороне многоканальной системы сообщения от каждого из источников информации модулируют по какому-либо параметру выделенные данному источнику канальные сигналы. Затем промодулированные канальные сигналы объединяются по тому или иному правилу, в результате чего формируется суммарный (групповой) сигнал. Данная операция называется *уплотнением каналов*. Полученный групповой сигнал затем модулирует несущее колебание, которое поступает на передачу. При использовании общей несущей канальные сигналы иногда называют *поднесущими* колебаниями. В ряде случаев, когда источники информации территориально сосредоточены, общая несущая не используется и канальные сигналы формируются непосредственно на несущих частотах. На приемной стороне многоканальной радиолинии после демодуляции несущей осуществляется операция, обратная операции уплотнения – из группового сигнала выделяются сигналы отдельных каналов. Данная операция называется *разделением (селекцией) каналов* [2].