УДК 621.372.037.372;621.391.26

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

кан. техн. наук Д.С. РЯБЕНКО, С.В. ЛАВРОВ, Е.С. БОРОВКОВА
(Полоцкий государственный университет)

Оценка напряженности магнитного поля является одной из важных задач для определения утечки информации. По результирующему вектору напряженности информационного магнитного поля определяют величину и направление сигнала, формируемого парциальными неориентированными излучателями. В работе использован матрично-топологический метод для определения направления и величины информационных сигналов, а следовательно, и напряженности магнитного поля.

Ключевые слова: *сигнальные графы, матрица, информационный сигнал.*

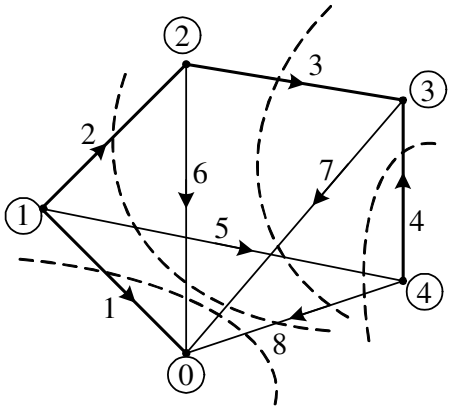
Высокая степень интеграции микроэлектроники, стремительное развитие технологических и информационных процессов обусловили новые принципиальные решения защиты информации от утечки. Физические и математические модели устанавливают рациональные методы исследования сложных информационных систем на всех стадиях их жизненного цикла и их элементов (блоки, печатные платы). Показатели защищенности оценивают в условиях активной и пассивной защиты каждого канала утечки информации [1].

Для получения достоверной информации нами использованы численные методы нахождения токов в различных цепях электронных приборов. При определении информационного сигнала в различных элементах электрической цепи используют матрично-топологический метод. Анализ электронных схем производят с помощью топологического описания цепи и математической модели, которая представляет собой систему уравнений, описывающих работу исследуемой схемы.

В основе топологического описания схем лежит понятие графа. Описание реальных объектов с помощью графов встречается весьма часто и применяется в самых разных областях знаний. Анализ теории графов указывает на необходимость представления графа в виде матрицы смежности и матрицы инциденций.

Дуги графа, моделирующего электрическую цепь, интерпретируются как сопротивление или проводимость, а также как источники тока или напряжения. В вершинах графа происходит разветвление (слияние) токов [2]. Под графом G понимают пару (V, Γ), где V – множество вершин, Γ – множество ребер [3].

Рассмотрена электрическая цепь, по которой построен граф, представленный на рисунке 1. Построение графа производится по эквивалентной схеме, которую получают из принципиальной электрической схемы. Для преобразования последней все нелинейные элементы, такие как диоды и транзисторы, заменяют их упрощенными эквивалентными схемами.



0–4 – узлы графа; --- – главные сечения графа;
1–8 – ребра графа (1–4 – ветви, 5–7 – хорды)
Рисунок 1. – Прохождение сигнала в электрической цепи

Любой граф, изображенный в геометрической форме в виде точек и соединяющих их дуг, может быть представлен в эквивалентной матричной форме [2]. Одной из матричных форм представления графа является матрица смежности. Порядок матрицы $n \times n$, где n – число вершин графа, элементы матрицы $a_{ij} = 1$, если дуга $\in \Gamma$, $a_{ij} = 0$, если дуга $\notin \Gamma$ [3]. Составим матрицу смежности представленного графа

$$A_C = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \left| \begin{array}{ccccc} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{array} \right| \end{array}. \quad (1)$$

Недостатком матрицы смежности является тот факт, что независимо от числа ребер объем занятой памяти составляет n^2 [4].

Другой матричной формой представления графа является матрица инциденций. Размерность матрицы $n \times m$, где n – число вершин, m – число дуг графа. Каждой i-й строке матрицы инциденций поставлена в соответствие вершина графа (ν_i) и каждому j-му столбцу матрицы инциденций – дуга графа (u_j). Элемент b_{ij} матрицы инциденций равен –1, если в вершину ν_i заходит дуга u_j; равен +1, если из вершины ν_i исходит дуга u_j, и равен 0, если дуга u_j и вершина ν_i не являются инцидентнми [5]. Тогда матрица инциденций примет вид

$$A_И = \begin{vmatrix} -1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 \end{vmatrix}. \quad (2)$$

Однако для анализа электронных схем переводить информацию, содержащуюся в графе, на алгоритмический язык проще и наглядней с помощью топологических матриц: матрицы главных сечений графа, матрицы главных контуров и структурной матрицы графа [5]. Сечением графа называется линия, делящая граф на две несвязанные части. Для получения главного сечения графа нужно линию сечения графа провести таким образом, чтобы она пересекала только одну ветвь при произвольном пересечении хорд. Построим матрицу главных сечений

$$A_{сеч} = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 \end{vmatrix}. \quad (3)$$

Каждый элемент матрицы $a_{ij} = +1$, если j-е ребро пересекает i-е сечение в том же направлении, что и ветвь, определяющая это сечение, и $a_{ij} = -1$, если j-е ребро пересекает i-е сечение в направлении, противоположном направлению ветви, определяющей это сечение, $a_{ij} = 0$, если j-е ребро не пересекает i-е сечение [5].

Сформированная матрица состоит из двух подматриц

$$A_{сеч} = |E, F|,$$

где E – единичная матрица главных сечений для ветвей, F – матрица главных сечений для хорд.

Матрицу главных сечений $A_{сеч}$ можно использовать для записи уравнений по первому закону Кирхгофа, тогда система будет иметь вид

$$\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \\ i_5 \\ i_6 \\ i_7 \\ i_8 \end{vmatrix} = 0 \qquad (4)$$

или

$$\mathrm{A}_{\text{сеч}} \cdot \mathbf{I} = 0 ,$$

где $\mathbf{I}$ – вектор-столбец токов ребер, который состоит из двух подвекторов, один из которых вектор токов ветвей $\mathbf{I}_\mathrm{B}$, а другой – вектор токов хорд $\mathbf{I}_\mathrm{X}$:

$$\mathbf{I} = \begin{vmatrix} i_1 & i_2 & i_3 & i_4 & i_5 & i_6 & i_7 & i_8 \end{vmatrix}^\mathrm{T} = \begin{vmatrix} \mathbf{I}_\mathrm{B} \\ \mathbf{I}_\mathrm{X} \end{vmatrix} .$$

Тогда уравнение (4) преобразуется к виду

$$\mathrm{A}_{\text{сеч}} \cdot \mathbf{I} = \begin{vmatrix} \mathrm{E}, \mathrm{F} \end{vmatrix} \cdot \begin{vmatrix} \mathbf{I}_\mathrm{B} \\ \mathbf{I}_\mathrm{X} \end{vmatrix} = \mathrm{E} \cdot \mathbf{I}_\mathrm{B} + \mathrm{F} \cdot \mathbf{I}_\mathrm{X} = \mathrm{F} \cdot \mathbf{I}_\mathrm{X} + \mathbf{I}_\mathrm{B}$$

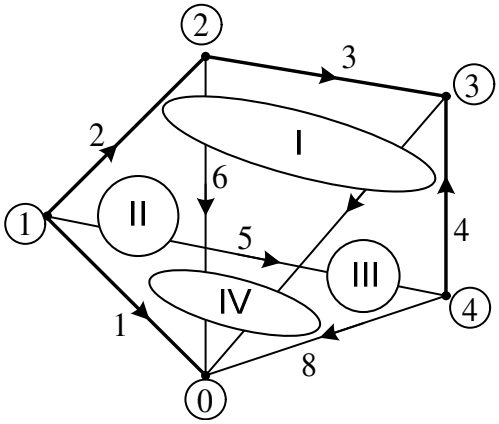
или

$$\mathbf{I}_\mathrm{B} = -\mathrm{F} \cdot \mathbf{I}_\mathrm{X} . \qquad (5)$$

С учетом (5) запишем зависимость

$$\begin{vmatrix} i_1 \\ i_2 \\ i_3 \\ i_4 \end{vmatrix} = \begin{vmatrix} 0 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 \end{vmatrix} \cdot \begin{vmatrix} i_5 \\ i_6 \\ i_7 \\ i_8 \end{vmatrix} . \qquad (6)$$

Построим матрицу главных контуров, для этого нанесем на граф линии главных контуров, представленные на рисунке 2.



I–IV – главные контуры графа
Рисунок 2. – Граф с линиями главных контуров

$$\mathrm{A}_{\text{конт}} = \begin{vmatrix} 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{vmatrix}. \quad (7)$$

Каждый элемент матрицы $a_{ij} = +1$, если направление j-го ребра совпадает с направлением главного контура, $a_{ij} = -1$ – если направление j-го ребра противоположно направлению главного контура и $a_{ij} = 0$ – если j-е ребро не образует главного контура.

Сформированная матрица состоит из двух подматриц

$$\mathrm{A}_{\text{конт}} = \left| -\mathrm{F}^{\mathrm{T}}, \mathrm{E} \right|.$$

Используя второй закон Кирхгофа, с учетом (7) система уравнений

$$\begin{vmatrix} 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{vmatrix} \cdot \begin{vmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \\ u_5 \\ u_6 \\ u_7 \\ u_8 \end{vmatrix} = 0 \quad (8)$$

или

$$\mathrm{A}_{\text{конт}} \cdot \mathbf{U} = 0,$$

где **U** – вектор-столбец напряжений, который состоит из двух подвекторов:

$$\mathbf{U} = \left| u_1 \quad u_2 \quad u_3 \quad u_4 \quad u_5 \quad u_6 \quad u_7 \quad u_8 \right|^{\mathrm{T}} = \begin{vmatrix} \mathbf{U}_{\mathrm{B}} \\ \mathbf{U}_{\mathrm{X}} \end{vmatrix}.$$

Тогда уравнение (8) преобразуется к виду

$$\mathrm{A}_{\text{конт}} \cdot \mathbf{U} = \left| -\mathrm{F}^{\mathrm{T}}, \mathrm{E} \right| \cdot \begin{vmatrix} \mathbf{U}_{\mathrm{B}} \\ \mathbf{U}_{\mathrm{X}} \end{vmatrix} = -\mathrm{F}^{T} \cdot \mathbf{U}_{\mathrm{B}} + \mathbf{U}_{\mathrm{X}}$$

или

$$\mathbf{U}_{\mathrm{X}} = \mathrm{F}^{\mathrm{T}} \cdot \mathbf{U}_{\mathrm{B}}. \quad (9)$$

С учетом (9) запишем зависимость

$$\begin{vmatrix} u_5 \\ u_6 \\ u_7 \\ u_8 \end{vmatrix} = \begin{vmatrix} 0 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 \end{vmatrix} \cdot \begin{vmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{vmatrix}.$$

Топологическим уравнением цепи называют матричное уравнение, объединяющее (5) и (9)

$$\begin{vmatrix} \mathbf{I}_{\mathrm{B}} \\ \mathbf{U}_{\mathrm{X}} \end{vmatrix} = \begin{vmatrix} -\mathrm{F} & 0 \\ 0 & \mathrm{F}^{T} \end{vmatrix} \cdot \begin{vmatrix} \mathbf{I}_{\mathrm{X}} \\ \mathbf{U}_{\mathrm{B}} \end{vmatrix}.$$

Далее данное уравнение преобразуется к виду для независимых источников тока и напряжения. Зная величину и направление информационных сигналов, определяется вектор магнитной напряженно-

сти от каждого элемента электрической цепи, после чего находится результирующий вектор и его величина с помощью корреляционного метода.

Распределение магнитных информационных полей рассеивания с выделением результирующего вектора реализует алгоритмы для оценки защищенности информации в каналах утечки и их наводок на неинформативные цепи.

Авторы благодарят доктора технических наук, профессора В.К. Железняка за научную консультацию при выполнении исследовательской работы.

ЛИТЕРАТУРА

1. Железняк В.К. Защита информации от утечки по техническим каналам : учеб. пособие / В.К. Железняк. – СПб. : ГУАП, 2006. – 188 с.
2. Куликовский, Л.Ф. Теоретические основы информационных процессов : учеб. пособие для вузов по специальности «Автоматизация и механизация процессов обработки и выдачи информации» / Л.Ф. Куликовский, В.В. Мотов. – М. : Высш. шк.,1987. – 248 с.
3. Корни, Ш. Теория цепей. Анализ и синтез / Ш. Корни. – М. : Связь, 1973. – 308 с.
4. Липский, В. Комбинаторика для программистов : пер. с пол. / В. Липский. – М. : Мир, 1988. – 213 с.
5. Лосев, А.К. Теория линейных электрических цепей : учеб. для вузов / А.К. Лосев. – М. : Высш. шк., 1987. – 512 с.
6. Демидович, Б.П. Основы вычислительной математики : учеб. пособие для студентов высш. техн. учеб. заведений / Б.П. Демидович, П.А. Марон. – М. : Наука, 1970. – 664 с.
7. Марпл-мл., С.Л. Цифровой спектральный анализ и его приложения / С.Л. Марпл-мл. – М. : Мир, 1990. – 584 с.
8. Андерсон, Т. Введение в многомерный статистический анализ / Т. Андерсон. – М. : Физматгиз, 1963. – 500 с.

Поступила 20.03.2018

THE APPLICATION OF SIGNAL GRAPHS AND MATRIX ANALYSIS FOR MATHEMATICAL MODELING CHANNELS OF INFORMATION LEAKAGE

D. RYABENKO, S. LAVROV, Y. BARAUKOVA

Estimation of magnetic field intensity is one of the important tasks for determination of information leakage. The resulting vector of the information magnetic field intensity determines the magnitude and direction of the signal generated by partial undirected emitters. In this paper, a matrix-topological method is used to determine the direction and magnitude of information signals, and hence the magnetic field strength.

Keywords: *signal graphs, matrix, information signal.*