УДК 621.372.037.372; 621.391.26

ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ КОРРЕЛЯЦИОННО-МАТРИЧНОЙ ОБРАБОТКОЙ ДАННЫХ

Е.С. БОРОВКОВА, В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО, С.В. ЛАВРОВ

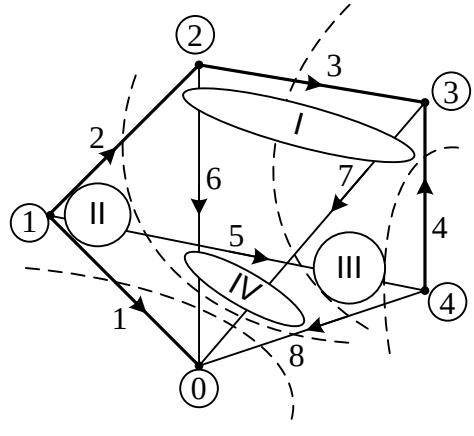
Полоцкий государственный университет

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].

Одной из важных задач по определению утечки информации в различных электронных приборах, как правило, требуется определить напряженность магнитного поля. При этом возникает сложность в нахождении результирующего вектора напряженности в переменном магнитном поле. В таких случаях важно определить величину и направление информационного сигнала, проходящего через элементы информационных цепей, и по имеющимся данным определить суммарный вектор магнитного поля. В данной работе использован матрично-топологический метод для определения направления и величины информационных сигналов, а следовательно, и магнитной напряженности.

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.



0 – 4 – узлы графа;
--- – главные сечения графа;
1 – 8 – ребра графа (1 – 4 – ветви, 5 – 7 – хорды);
I – IV – главные контуры графа.

Рис. 1. Прохождение сигнала в схеме.

Рассмотрена электрическая цепь, по которой построен граф, представленный на рисунке 1. Предполагается, что схемные элементы работают в линейном режиме.

Анализ электронных схем реализует с помощью топологических матриц, а именно матрицы главных сечений графа, матрицы главных контуров и структурной матрицы графа [5].

Построена матрица главных сечений (рис. 1)

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

Сформированная матрица состоит из двух подматриц $\mathrm{A}_{сеч} = |\mathrm{E}, \mathrm{F}|$, где E – единичная матрица главных сечений для ветвей, F – матрица главных сечений для хорд. Используя первый закон Кирхгофа $\mathrm{A}_{сеч} \cdot \mathbf{I} = 0$, получают зависимость

$$\mathrm{A}_{сеч} \cdot \mathbf{I} = |\mathrm{E}, \mathrm{F}| \cdot \begin{vmatrix} \mathbf{I}_B \\ \mathbf{I}_X \end{vmatrix} = \mathrm{E} \cdot \mathbf{I}_B + \mathrm{F} \cdot \mathbf{I}_X = \mathrm{F} \cdot \mathbf{I}_X + \mathbf{I}_B, \quad (2)$$

или $\mathbf{I}_B = -\mathrm{F} \cdot \mathbf{I}_X$,

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

С учетом (2) представляют систему уравнений в матричном виде

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

Матрица главных контуров, согласно рис. 1 имеет вид:

$$\mathrm{A}_{конт} = \begin{vmatrix} 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{vmatrix}. \quad (3)$$

Используя второй закон Кирхгофа $\mathrm{A}_{конт} \cdot \mathbf{U} = 0$, получают зависимость

$$\mathrm{A}_{конт} \cdot \mathbf{U} = |-\mathrm{F}^{\mathrm{T}}, \mathrm{E}| \cdot \begin{vmatrix} \mathbf{U}_B \\ \mathbf{U}_X \end{vmatrix} = -\mathrm{F}^T \cdot \mathbf{U}_B + \mathbf{U}_X, \quad (4)$$

либо в сокращенном виде $\mathbf{U}_X = \mathrm{F}^{\mathrm{T}} \cdot \mathbf{U}_B$.

С учетом (4) записывается 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 (2) и (4)

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

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

Список литературы

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