ОЦЕНКА ЗАЩИЩЕННОСТИ РЕЧЕВОЙ ИНФОРМАЦИИ КОРРЕЛЯЦИОННО-МАТРИЧНОЙ ОБРАБОТКОЙ ДАННЫХ

Железняк В.К.; Рябенко Д.С.; Лавров С.В.; Боровкова Е.С.

2018

Математическое описание колебаний сложной системы для оценки защиты информации является весьма трудоемкой задачей из-за несовершенства схемно-конструктивных решений элементов сложных систем, подверженных динамическим воздействиям, снижающих качество функционирования. Разработка сложных систем без исследования требований, повышающих качество защиты информации на всех стадиях жизненного цикла, является актуальной задачей.

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

Предложена оценка защищенности каналов утечки векторным геометрическим представлением сигналов корелляционно-регрессионным линейным анализом на основании методов обработки статистических данных парной корреляции, частной корреляции и множественной корреляции.

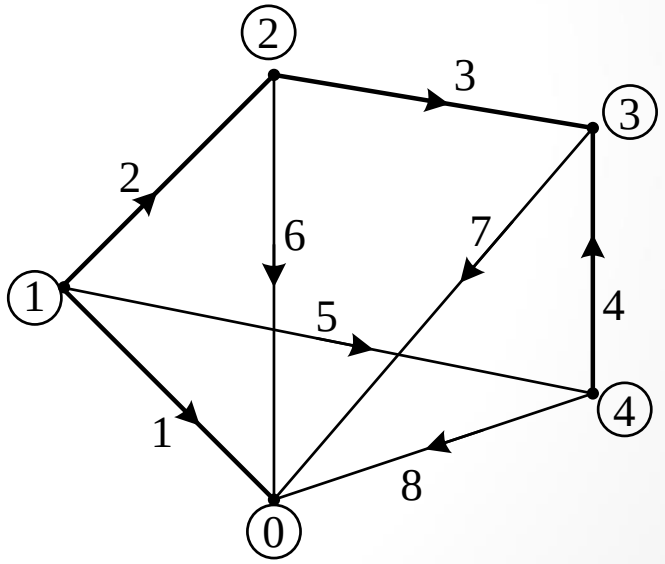
Понятие графа

В основе топологического описания схем лежит понятие графа.

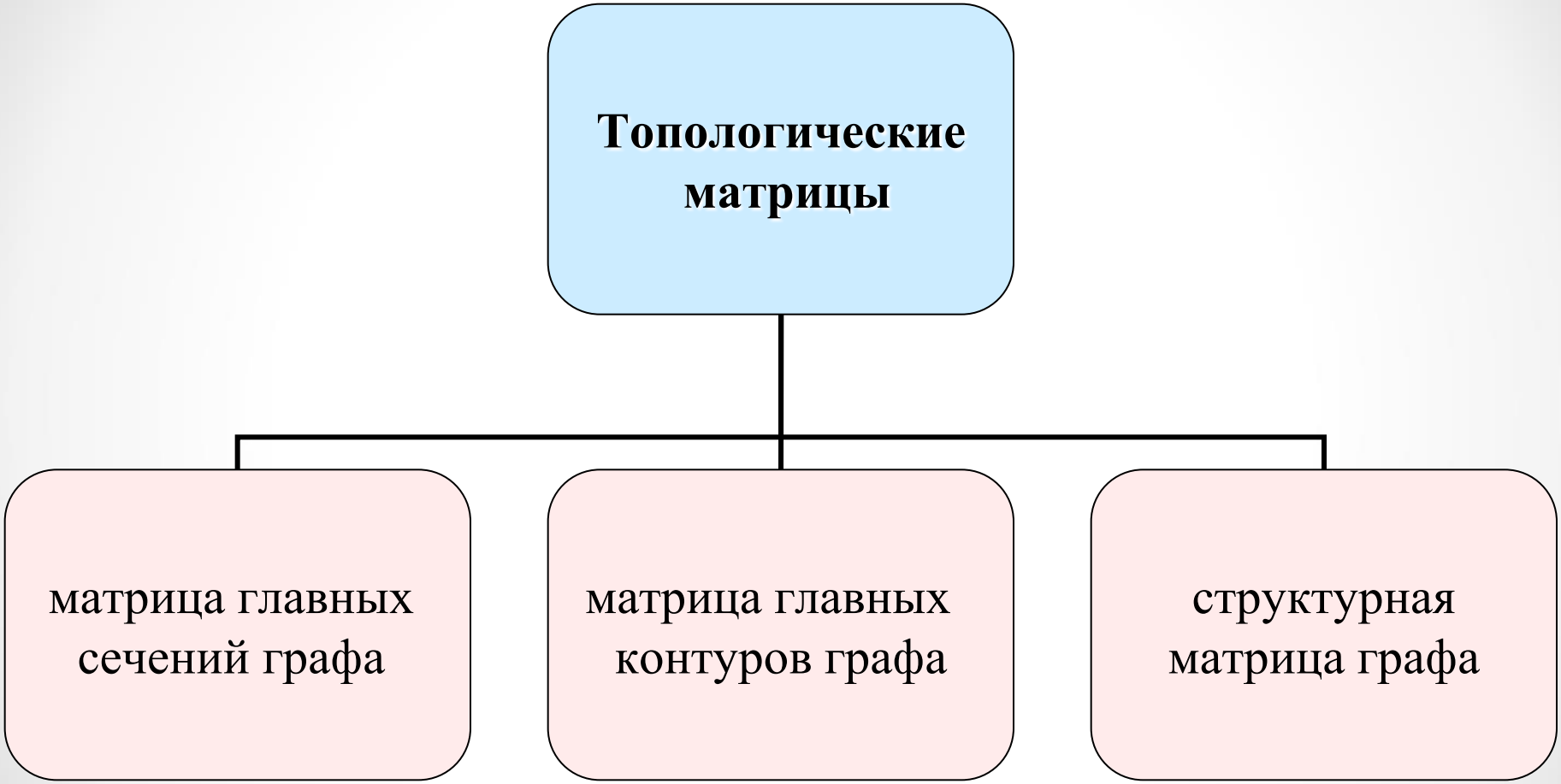
Дуги графа, моделирующего электрическую цепь, интерпретируются как сопротивление или проводимость, а также как источники тока или напряжения. В вершинах графа происходит разветвление (слияние) токов. Под графом G понимают пару (V, Γ), где V – множество вершин, Γ – множество ребер.

Приложение сигнальных графов

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.

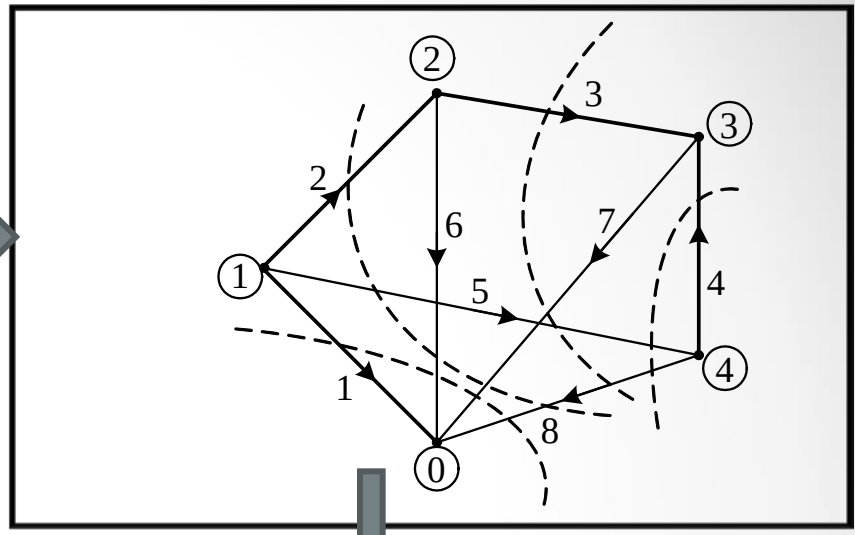


Прохождение сигнала в схеме.


Топологические матрицы
матрица главных сечений графа
матрица главных контуров графа
структурная матрица графа

Матрица главных сечений

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.



Каждый элемент a_{ij} матрицы равен: $a_{ij} = +1$, если j-е ребро пересекает i-е сечение в том же направлении, что и ветвь, определяющая это сечение, $a_{ij} = -1$, 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.

$$A_{сеч} = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 1 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 1 \end{vmatrix}$$

$$A_{сеч} = |E, F|$$

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

Лосев А.К. Теория линейных электрических цепей: Учеб. для вузов. – М.: Высш. шк., 1987. – 512 с.

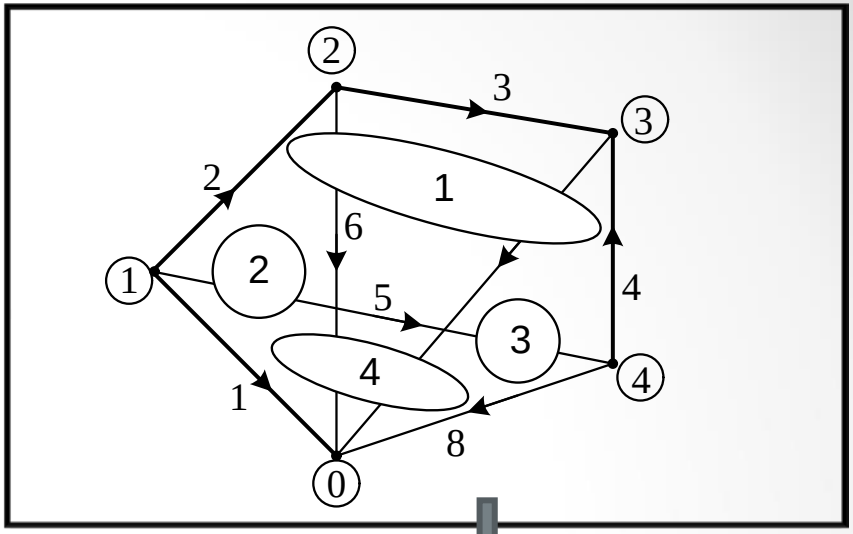
Матрица главных сечений

$$A_{сеч} \cdot \mathbf{I} = \left|E, F\right| \cdot \begin{vmatrix} \mathbf{I}_B \\ \mathbf{I}_X \end{vmatrix} = E \cdot \mathbf{I}_B + F \cdot \mathbf{I}_X = F \cdot \mathbf{I}_X + \mathbf{I}_B \Rightarrow \mathbf{I}_B = -F \cdot \mathbf{I}_X$$

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

Матрица главных контуров графа

Каждый элемент a_{ij} матрицы равен: 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, a_{ij} = 0, если j-е ребро не образует главного контура.



$$A_{конт} = \begin{vmatrix} 0 & -1 & -1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ -1 & 1 & 1 & -1 & 0 & 0 & 0 & 1 \end{vmatrix}$$

$$A_{конт} = \left| -F^{T}, E \right|$$

Матрица главных контуров

$$A_{конт} \cdot \mathbf{U} = \left| -F^{T}, E \right| \cdot \begin{vmatrix} \mathbf{U}_B \\ \mathbf{U}_X \end{vmatrix} = -F^{T} \cdot \mathbf{U}_B + \mathbf{U}_X \quad \Rightarrow \quad \mathbf{U}_X = F^{T} \cdot \mathbf{U}_B$$

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

структурная матрица графа

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

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.

Метод корреляционной обработки сигнала

Одним из методов обработки аналоговых и цифровых сигналов для оценки защиты речевой информации остается корреляционный метод

Корреляционная функция периодических процессов характеризует взаимную связь двух мгновенных значений различных сигналов с временным сдвигом τ .

Взаимная корреляционная функция для двух действительных периодических процессов с одинаковой основной частотой

$$R_{v_1 v_2}(\tau) = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} v_1(t) v_2(t+\tau)\,\mathrm{d}t.$$

Коэффициент взаимной корреляции

$$r(v_1, v_2) = \frac{R_{v_1 v_2}}{\sigma_{v_1}\sigma_{v_2}} = \frac{R_{v_1 v_2}}{\sqrt{R(v_1 \cdot v_1) \cdot R(v_2 \cdot v_2)}},$$

где $R_{v_1 v_2}$ – взаимная корреляционная функция; σ^2 – дисперсия.

Коэффициент множественной корреляции

Нормированная корреляционная матрица, т.е. матрица коэффициентов корреляции, для системы случайных величин $\{X_1, X_2, X_3, ..., X_n\}$

$$\|r_{ij}\| = \begin{Vmatrix} 1 & r_{12} & r_{13} & \dots & r_{1n} \\ r_{21} & 1 & r_{23} & \dots & r_{2n} \\ r_{31} & r_{32} & 1 & \dots & r_{3n} \\ . & . & . & . & . \\ r_{n1} & r_{n2} & r_{n3} & \dots & 1 \end{Vmatrix}$$

Коэффициент множественной корреляции используется для описания системы случайных величин $\{X_1, X_2, X_3, ..., X_n\}$

Служит характеристикой корреляции между случайной величиной X_1 и совокупностью случайных величин $(X_2, X_3, ..., X_n)$

Метод корреляционной обработки сигнала

Распределение системы n случайных величин представимы в виде n – мерного случайного вектора с составляющими.
Его плотность записывается в виде

$$f(x_1,\ldots,x_n)=\frac{1}{(2\pi)^{n/2}\sqrt{\Delta}}\exp\left\{-\frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n}K_{ij}^{(-1)}(x_i-m_i)(x_j-m_j)\right\}$$

m_i - математическое ожидание величины x_i (i = 1,2,…,n);

Δ - определитель ковариационной матрицы $\|K_{ij}\|$ системы случайных величин $(X_1, X_2, X_3,\ldots, X_n)$:

Коэффициенты парной корреляции

Коэффициенты парной корреляции используются для измерения линейных связей различных пар из их множества. При этом учитывается, что связь каждой пары находится под воздействием связей всех других признаков между собой и с признаками из данной пары.

Матрицу парных корреляций *R* получают путем преобразования матрицы исходных данных *X*

$$X \to Z \to Z'Z \to \frac{1}{n} Z'Z = R$$

$$z_{ij} = \frac{x_{ij} - \overline{x}_j}{\sigma_j} \qquad Z = \left\| z_{ij} \right\|$$

Коэффициенты частной корреляции

Коэффициенты частной корреляции представляют линейные связи признаков, при этом принимается чистая связь пары признаков при условии, что связи всех других признаков с признаками из данной пары не действуют, нивелированы. Элементы матрицы коэффициентов частной корреляции получают по данным известной матрицы парных корреляций R

$$r_{ij} = -\frac{A_{ij}}{(A_{ii}A_{jj})^{1/2}}$$

A_{ij}, A_{jj}, A_{ii} – алгебраические дополнения к соответствующим элементам матрицы парных корреляций R.

Заключение

Информационные связи должны исследоваться с целью их снижения для установления однозначной линейной связи между величинами. Только таким образом можно установить различные связи напряженности магнитных полей, а зная их добиться, чтобы между информационной цепью и цепью, на которую наводится сигнал не было корреляционных связей.

Выводы

Матрично-топологический метод позволяет определить информационный сигнал в различных элементах электрической цепи

Корреляционно-матричная обработка схемно-конструктивных решений радиоэлектронных систем реализует оценку защищенности речевой информации по магнитным информационным полям рассеивания, наведенным на неинформационные цепи (управления, питания, заземления), в соответствии с установленным нормативным численным значением. Системный анализ усложняется необходимостью разработки элементов проблемных решений для получения результатов с заданной точностью при значительных диапазонах влияющих факторов.

Спасибо за внимание