Міністерство освіти й науки України
Одеський національний морський університет

КОБОЗЄВА АЛЛА АНАТОЛІЇВНА

ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ТА СУЧАСНІ ПІДХОДИ ДО ЇХ ВИРІШЕННЯ

Конспект лекцій

для здобувачів
другого (магістерського) рівня вищої освіти
спеціальності F5 Кібербезпека та захист інформації
галузі знань F Інформаційні технології

Одеса-2025

Розробник: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідувач кафедри «Кібербезпека та захист інформації»

Конспект лекцій схвалено на засіданні кафедри «Кібербезпека та захист інформації»
(Протокол від «06» жовтня 2025 р. №2)

Конспект лекцій схвалено на засіданні НМК ННІ ІТІП
(Протокол від «14» жовтня 2025 р. № 2)

ЗМІСТ

ТЕМА 1. МАТРИЧНІ РОЗКЛАДАННЯ

План

1. Деякі визначення й поняття лінійної алгебри
2. *LU*-розкладання матриці й заснований на ньому метод розв'язку системи лінійних рівнянь
3. Розкладання симетричної додатно визначеної матриці
4. Поняття власного значення й власного вектора матриці
5. Властивості власних значень і власних векторів матриці. Теорема про спектральне розкладання матриці
6. Теорема про сингулярне розкладання матриці
7. Поняття чутливості задачі
8. Чутливість власних значень (сингулярних чисел) і власних векторів (сингулярних векторів) до збурних дій

1. Деякі визначення й поняття лінійної алгебри

Визначення. Нехай V - деякий векторний простір. Функція

$$\|\bullet\| : V \to R$$

називається *векторною нормою*, якщо для $\forall x, y \in V$ виконуються наступні умови:

1. $\|x\| \geq 0$ - *невід'ємність*; при цьому
$$\|x\| = 0 \quad \Leftrightarrow \quad x = 0 .$$
2. $\forall c \in R : \|cx\| = |c|\|x\|$ - *однорідність*;
3. $\|x + y\| \leq \|x\| + \|y\|$ - *нерівність трикутника*.

Приклади векторних норм.

Вектор $x = (x_1, x_2, ..., x_n)^T$.

1. $\|x\|_1 = |x_1| + |x_2| + ... + |x_n|$ - перша векторна норма;
2. $\|x\|_\infty = max\{|x_1|, |x_2|, ..., |x_n|\}$ - l_∞-норма;
3. $\|x\|_p = \left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}, \quad p \geq 1$ - l_p-норма чи норма Гьольдера з показником p.

Визначення. Нехай M_n - матричний простір (матриці розміром $n \times n$). Функція

$$\|\bullet\| : M_n \to R$$

називається *нормою матриці*, якщо $\forall A, B \in M_n$ виконуються наступні умови:

1. $\|A\| \geq 0$ - *невід'ємність*; при цьому
$$\|A\| = 0 \quad \Leftrightarrow \quad A = 0 .$$

2. $\forall c \in R: \|cA\| = |c|\|A\|$ - *однорідність*;
3. $\|A + B\| \le \|A\| + \|B\|$ - *нерівність трикутника*;
4. $\|AB\| \le \|A\| \cdot \|B\|$ - *кільцева властивість*.

Приклади матричних норм.

1. $\|A\|_F = \sqrt{\sum_{i,j=1}^{n} |a_{ij}|^2}$ - норма Фробеніуса;
2. $\|A\|_{max} = \max_{i,j} |a_{ij}|$ - max-норма;
3. $\|A\|_{\infty} = \max_{i} \sum_{j=1}^{n} |a_{ij}|$;
4. $\|A\|_1 = \max_{j} \sum_{i=1}^{n} |a_{ij}|$;
5. $\|A\|_2 = \sqrt{\lambda_{max}(A^* A)}$ - спектральна матрична норма, де $\lambda_{max}(A^* A)$ - максимальне власне значення матриці $A^* A$.

2. *LU*-розкладання матриці

Нехай A - $n \times n$ – матриця з дійсними елементами a_{ij}, $i, j = \overline{1,n}$.

Розкладанням матриці A називається її представлення у вигляді добутку декількох «більш простих» матриць, що полегшує розв'язок задачі, що розглядається.

Теорема. Нехай усі головні підматриці $A^{(k)}$, $k = 1,..., n$, матриці A є невиродженими. Тоді A єдиним чином представляється у вигляді:

$$A = LU, \qquad (1.1)$$

де L - нижня трикутна матриця з одиницями на головній діагоналі, U - верхня трикутна матриця, діагональні елементи якої визначаються по формулі:

$$u_{kk} = \frac{det\, A^{(k)}}{det\, A^{(k-1)}}, \quad k = 1,..., n, \quad det\, A^{(0)} = 1.$$

Представлення (1.1) називається *LU*-розкладанням матриці A.

Доказ. Доказ проведемо конструктивно, тобто побудуємо безпосередньо розкладання (1.1). Нагадаємо, що головні підматриці A - це

$$A=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2,n-1} & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3,n-1} & a_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \dots & a_{n-1,n-1} & a_{n-1,n} \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{n,n-1} & a_{nn} \end{pmatrix}$$

$$\Downarrow$$

$$A^{(1)}=\begin{pmatrix} a_{11} \end{pmatrix},\ A^{(2)}=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},\ A^{(3)}=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

$$\dots,\ A^{(n-1)}=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1,n-1} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2,n-1} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3,n-1} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \dots & a_{n-1,n-1} \end{pmatrix},$$

$$A^{(n)}=\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1,n-1} & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2,n-1} & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3,n-1} & a_{3n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \dots & a_{n-1,n-1} & a_{n-1,n} \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{n,n-1} & a_{nn} \end{pmatrix}.$$

Припустимо, що розкладання (1.1) вже побудовано, тобто матриця A представлена в вигляді:

$$\begin{array}{ccccc} A & = & L & \cdot & U \\ \downarrow & & \downarrow & & \downarrow \end{array}$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ l_{21} & 1 & 0 & \dots & 0 \\ l_{31} & l_{32} & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ l_{n1} & l_{n2} & l_{n3} & \dots & 1 \end{pmatrix}\cdot\begin{pmatrix} u_{11} & u_{12} & u_{13} & \dots & u_{1n} \\ 0 & u_{22} & u_{23} & \dots & u_{2n} \\ 0 & 0 & u_{33} & \dots & u_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & u_{nn} \end{pmatrix}$$

Елементи матриці A відомі, а елементи матриць L,U необхідно знайти. Побудуємо систему рівнянь щодо невідомих елементів матриць L,U, записуючи рівняння для відповідних елементів матриці A:

$$\sum_{j=1}^{n} l_{ij} u_{jk} = a_{ik}, \quad i,k = \overline{1,n} \tag{1.2}$$

чи, враховуючи, що

$$l_{ij} = 0 \quad при \quad i < j,$$

$$u_{jk} = 0 \quad при \quad k < j$$

систему (1.2) можна записати в вигляді:

$$\left(\sum_{j=1}^{min(i,k)} l_{ij} u_{jk} = a_{ik}, \quad i,k = \overline{1,n} \right) \quad \Leftrightarrow \quad \left(\begin{array}{ll} \sum_{j=1}^{k} l_{ij} u_{jk} = a_{ik}, & при \quad k \le i \\ \sum_{j=1}^{i} l_{ij} u_{jk} = a_{ik}, & при \quad i < k \end{array} \right). \tag{1.3}$$

Записуючи послідовно рівняння системи (1.2), отримаємо:
для a_{11}, враховуючи, що цей елемент ми отримуємо при множенні першого рядка матриці L на перший стовпець матриці U:

$$a_{11} = u_{11},$$

звідки відразу отримуємо значення для $u_{11} = a_{11}$.
Елемент a_{12} ми отримуємо як результат множення першого рядка матриці L на другий стовпець матриці U:

$$a_{12} = u_{12},$$

звідки $u_{12} = a_{12}$.
Ідучи послідовно по елементах першого рядка матриці A, отримаємо, що

$$u_{1i} = a_{1i}, \quad i = 1,..., n.$$

Переходимо на другий рядок матриці A:

$$a_{21} = l_{21} u_{11} \quad \overset{враховуючи, що\ u_{11}\ вже відомо}{\Rightarrow} \quad l_{21} = \frac{a_{21}}{u_{11}}.$$

$$a_{22} = l_{21} u_{12} + u_{22} \quad \overset{враховуючи, що\ u_{12}, l_{21}\ вже відомі}{\Rightarrow} \quad u_{22} = a_{22} - l_{21} u_{12},$$

і т.д. Проводячи обчислення, складаючи рівняння для елементів матриці A у порядку

$$(i,k) = (1,1),...,(1,n),(2,1),...,(2,n),(3,1),...,(3,n),...,(n,1),...,(n,n),$$

отримаємо наступні формули для обчислення невідомих елементів матриць L,U:

$$u_{11} = a_{11},$$

$$u_{1j} = a_{1j}, \quad l_{j1} = \frac{a_{j1}}{u_{11}}, \quad j = 2,...,n,$$

$$u_{ii} = a_{ii} - \sum_{p=1}^{i-1} l_{ip} u_{pi}, \quad i = 2,...,n, \tag{1.4}$$

$$u_{ij} = a_{ij} - \sum_{p=1}^{i-1} l_{ip} u_{pj}, \quad l_{ji} = \frac{a_{ji} - \sum_{p=1}^{i-1} l_{jp} u_{pi}}{u_{ii}}, \quad i = 2,...,n, \quad j = i+2,...,n$$

Зрозуміло, що обчислення по формулах (1.4) можна проводити тільки тоді, коли $u_{ii} \neq 0, \quad i = 1,...,n$. Перевіримо виконання цієї умови. Із (1.3) випливає, що

$$A^{(k)} = L^{(k)} U^{(k)},$$

тому

$$det\left(A^{(k)}\right) = det\left(L^{(k)}\right) det\left(U^{(k)}\right). \tag{1.5}$$

Оскільки $L^{(k)}, U^{(k)}$ - нижня й верхня трикутні матриці відповідно, то їхні визначники дорівнюють добутку елементів, що знаходяться на головній діагоналі, тому

$$det\left(L^{(k)}\right) = 1, \quad det\left(U^{(k)}\right) = u_{11} u_{22} ... u_{kk},$$

і, як витікає з (1.5)

$$det\left(A^{(k)}\right) = u_{11} u_{22} ... u_{kk}.$$

За умовою теореми всі $A^{(k)}$, $k = 1,...,n$, є невиродженими, тобто

$$det\left(A^{(k)}\right) = u_{11} u_{22} ... u_{kk} \neq 0 \quad \Rightarrow \quad u_{ii} \neq 0, \quad i = 1,...,k,$$

крім того

$$u_{kk} = \frac{det\left(A^{(k)}\right)}{u_{11} u_{22} ... u_{k-1,k-1}} = \frac{det\left(A^{(k)}\right)}{det\left(A^{(k-1)}\right)},$$

що й потрібно було довести.

3. Розкладання симетричної додатно визначеної матриці

Нехай матриця A симетрична (тобто $A = A^T$) і додатно визначена.

Визначення. Матриця A називається ***додатно визначеною***, якщо для $\forall x \neq 0$ виконується:

$$x^T Ax > 0 .$$

Критерій Сильвестра додатної визначеності матриці. Для того, щоб матриця A розміру $n \times n$ була додатно визначеною, необхідно і достатньо, щоб визначники всіх її головних підматриць були додатними.

Теорема. Якщо A - симетрична й додатно визначена $n \times n$-матриця, то існує і єдино її трикутне розкладання $A = \overline{\overline{L}}\,\overline{\overline{L}}^T$, яке називається розкладанням Холеського, де $\overline{\overline{L}}$ - нижня трикутна матриця з додатними діагональними елементами.

Приклад. Потрібно побудувати розкладання Холеського для $\begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix}$.

Матриця $A = \begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix}$ є симетричною, оскільки $A = \begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix} = A^T$, і додатно визначеною (по критерію Сільвестра), оскільки

$$det\, A^{(1)} = det(6) = 6 > 0, \quad det\, A^{(2)} = det\begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix} = 47 > 0 .$$

Побудуємо для матриці A симетричне розкладання. Припустимо, що воно вже є:

$$\begin{array}{ccccc} A & = & \overline{\overline{L}} & \cdot & \overline{\overline{L}}^T \\ \downarrow & & \downarrow & & \downarrow \\ \begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix} & = & \begin{pmatrix} l_{11} & 0 \\ l_{21} & l_{22} \end{pmatrix} & & \begin{pmatrix} l_{11} & l_{21} \\ 0 & l_{22} \end{pmatrix} \end{array} .$$

Елемент $a_{11} = 6$ матриці A дорівнює добутку першого рядка матриці $\overline{\overline{L}}$ на перший стовпець матриці $\overline{\overline{L}}^T$, тобто $6 = l_{11}^2$, звідки $l_{11} = \sqrt{6}$. Елемент $a_{12} = 1$ матриці A дорівнює добутку першого рядка матриці $\overline{\overline{L}}$ на другий стовпець матриці $\overline{\overline{L}}^T$, тобто $1 = l_{11} l_{21}$, звідки $l_{21} = \dfrac{1}{l_{11}} = \dfrac{1}{\sqrt{6}}$. Елемент $a_{22} = 8$ матриці A дорівнює добутку другого рядка матриці $\overline{\overline{L}}$ на другий стовпець матриці $\overline{\overline{L}}^T$, тобто $8 = l_{21}^2 + l_{22}{}^2$, звідки $l_{22} = \sqrt{8 - l_{21}^2} = \sqrt{8 - \dfrac{1}{6}} = \sqrt{\dfrac{47}{6}}$. Таким чином:

$$\begin{pmatrix} 6 & 1 \\ 1 & 8 \end{pmatrix} = \begin{pmatrix} \sqrt{6} & 0 \\ \dfrac{1}{\sqrt{6}} & \sqrt{\dfrac{47}{6}} \end{pmatrix} \begin{pmatrix} \sqrt{6} & \dfrac{1}{\sqrt{6}} \\ 0 & \sqrt{\dfrac{47}{6}} \end{pmatrix}.$$

4. Поняття власного значення й власного вектора матриці

Визначення 1. Скаляр λ називається *власним значенням* (ВЗ), а вектор $\varphi \neq 0$ *власним вектором* (ВВ) матриці A, якщо виконується рівність:

$$A\varphi = \lambda\varphi . \qquad (1.6)$$

При цьому пара (λ, φ) називається власною парою матриці A.

Таким чином, власний вектор - це такий спеціальний вектор, який при множенні на матрицю A не змінює свого напрямку (при $\lambda > 0$) чи змінює на протилежне (при $\lambda < 0$).

Кожному власному значенню матриці відповідає нескінченно багато власних векторів. Дійсно, якщо φ - власний вектор A, що відповідає власному значенню λ (тобто виконується рівність (1.6)), то $c\varphi$, де $c \in R$, також є власним вектором A, що відповідає власному значенню λ. Дійсно:

$$A(c\varphi) = cA\varphi = \begin{bmatrix} A\varphi = \lambda\varphi, \\ т.к.\ (\lambda, \varphi) - \\ власна \\ пара\ A \end{bmatrix} = c\lambda\varphi = \lambda(c\varphi),$$

тобто за визначенням $(\lambda, c\varphi)$ - власна пара матриці A при $\forall c \in R$.

Визначення 2. Многочлен

$$det(A - \lambda E)$$

відносно скаляра λ називається ***характеристичним многочленом*** матриці A (тут E - одинична матриця відповідного розміру), а рівняння

$$det(A - \lambda E) = 0$$

характеристичним рівнянням.

Якщо матриця A має розміри $n \times n$, то характеристичний многочлен – це многочлен степеня n. Корені характеристичного рівняння - це власні значення матриці A, тому $n \times n$-матриця A має n однозначно визначених власних значень.

Визначення 3. Множина всіх власних значень матриці A називається її *спектром*.

5. Властивості власних значень і власних векторів матриці. Теорема про спектральне розкладання матриці

Перерахуємо деякі важливі властивості власних значень і власних векторів матриці.

1. Якщо матриця A самоспряжена (тобто $A = A^*$), то всі її власні значення дійсні, а значить усі власні значення можна перенумерувати по зростанню (можна по спаданню):
$$\lambda_1 \le \lambda_2 \le ... \le \lambda_n;$$

2. Якщо власні значення λ_i, λ_j матриці A різні, то відповідні їм власні вектори лінійно незалежні;

3. ***Спектральна теорема***. Нехай $n \times n$-матриця A симетрична, тобто $A = A^T$, тоді для неї можлива представлення у вигляді
$$A = U \Lambda U^T,$$
де $\Lambda = diag(\lambda_1,...,\lambda_n) = \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ ..... & & & \\ 0 & 0 & ... & \lambda_n \end{pmatrix}$ — діагональна матриця власних значень матриці A; $U = [\varphi_1,...,\varphi_n]$ — матриця, стовпці якої - це власні вектори матриці A, при цьому матриця U - ортогональна, тобто $UU^T = E$, де E - одинична матриця відповідного розміру. В загальному випадку спектральне розкладання визначається неоднозначно. СР назвемо нормальним, якщо елементи матриці Λ задовольняють співвідношенню: $|\lambda_1| \ge ... \ge |\lambda_n|$, а ВВ u_i, $i = \overline{1,n}$, лексикографічно додатні, при цьому вектор u називається лексикографічно додатним, якщо його перша ненульова компонента є додатною.

Теорема. Нехай F — невироджена симетрична $n \times n$-матриця, модулі ВЗ якої попарно різні. Тоді для неї існує єдине нормальне СР.

6. Теорема про сингулярне розкладання матриці

Нехай F — $m \times n$-матриця з елементами f_{ij}, $i = \overline{1,m}$, $j = \overline{1,n}$, ($m \ge n$). Для неї має місце розкладання, що називається ***сингулярним***:
$$F = U \Sigma V^T, \qquad (1.7)$$
де U, V — матриці розміру $m \times n$ і $n \times n$ відповідно, $\Sigma = diag(\sigma_1,...,\sigma_n)$, $\sigma_1 \ge ... \ge \sigma_n \ge 0$, при цьому U, V є ортогональними , тобто задовольняють співвідношенням: $U^T U = I$, $V^T V = I$, де I — одинична матриця відповідного розміру. Стовпці $u_1,...,u_n$ матриці U і $v_1,...,v_n$ матриці V називають відповідно лівими й правими сингулярними векторами (СНВ) матриці F, величини

$\sigma_1,...,\sigma_n$ — сингулярними числами (СНЧ), а (σ_i, u_i, v_i) сингулярними трійками F. При $m < n$ розглядається сингулярне розкладання матриці F^T.

Розкладання (1.7) може бути представлено у формі зовнішніх добутків:

$$F = \sum_{i=1}^{n} \sigma_i u_i v_i^T .$$

У загальному випадку сингулярне (спектральне) розкладання матриці визначається неоднозначно. Назвемо сингулярне розкладання (1.7) нормальним, якщо стовпці матриці U лексикографічно додатні.

Теорема. Невироджена матриця F має єдине нормальне сингулярне розкладання, якщо її СНЧ попарно різні:

$$\sigma_1 > ... > \sigma_n > 0 .$$

7. Чутливість задачі

При решении произвольной реальной задачи в общем случае невозможно получить точное значение искомого численного результата. Существование неустранимой погрешности в математической модели объекта или процесса, фигурирующего в задаче, погрешности входных данных, многие из которых в реальных условиях получены экспериментально, погрешность метода, используемого для решения, и вычислительная, погрешности, возникающие при каких-либо дополнительных воздействиях на объект, которые часто трактуются как возмущения входных данных, приводят к необходимости их совокупного учета при оценке погрешности результата. Даже в случае, когда входные данные математической модели не имеют погрешностей, а метод, выбранный для решения полученной математической задачи является точным, избежать вычислительной погрешности при проведении вычислений в системе чисел с плавающей точкой, а значит и погрешности в полученном результате, невозможно. Однако, в силу особенностей машинной арифметики, невозможно в общем случае получить точное решение даже смоделированной математической задачи (пренебрегая неустранимой погрешностью и погрешностью метода).

Полученное приближенное (в силу перечисленных выше причин) решение некоторой вычислительной задачи A может рассматриваться как точное решение, но другой, возмущенной задачи $\overline{A}$ ($\overline{A}$ отличается от A возмущением входных данных). В этом случае для определения качества полученного приближения необходимо иметь возможность оценить степень зависимости решения от возмущений исходных данных.

Некоторые вычислительные задачи очень сильно «реагируют» на даже малые изменения данных, причем это не зависит от системы с плавающей точкой или выбранного алгоритма, а является свойством самой задачи.

Пример. Рассмотрим квадратное уравнение, корни которого являются «почти» кратными:

$$(x-2)^2 = 10^{-6} .$$

Корни уравнения: $x = 2 \pm 10^{-3}$. Изменение правой части уравнения лишь на 10^{-6} вызовет изменение в корнях 10^{-3}, т.е. на три порядка большее, чем начальное. Рассмотренная задача является чувствительной.

Назвемо задачу ***чутливою*** до погрішностей вхідних даних, якщо навіть малі погрішності вхідних даних можуть привести до значної погрішності результату, і ***нечутливою*** інакше.

Для чувствительных задач «правильные» ответы (ответы с очень малой погрешностью) принципиально нельзя получить никаким алгоритмом, поскольку даже малые ошибки, допущенные при представлении данных и при вычислениях (а эти ошибки сопровождают вычислительный процесс всегда) приведут к значительным погрешностям в результатах. В силу этого чрезвычайно важной и актуальной является численная оценка такой чувствительности, установления параметров, определяющих чувствительность, достаточных условий нечувствительности задачи.

Нехай ξ — вхідні дані для деякої задачі, результатом розв'язку якої є $\phi(\xi)$; $\bar{\xi}$ — збурені вхідні дані, а розв'язок задачі, отриманий для цих вхідних даних, — $\phi(\bar{\xi})$. *Числом обумовленості* задачі називається величина, що визначається співвідношенням:

$$\overline{\lim_{\bar{\xi}\to\xi}} \frac{\textit{відстань між } \phi(\xi) \textit{ і } \phi(\bar{\xi})}{\textit{відстань між } \xi \textit{ і } \bar{\xi}}.$$

Очевидно, чим менше число обумовленості, тим менше збурення результату залежить від збурення вхідних даних, тим менше чутливість задачі, а при малому числі обумовленості задача виявиться нечутливою до погрішностей вхідних даних. Таким чином, ***число обумовленості задачі є її мірою чутливості до збурних дій***.

8. Чутливість власних значень (сингулярних чисел) і власних векторів (сингулярних векторів) до збурних дій

Нехай вхідна матриця F зазнала збурення ΔF, у результаті якого отримана матриця $F + \Delta F$. Для СНЧ $\sigma_j(F)$, $\sigma_j(F + \Delta F)$, $j = \overline{1,n}$, матриць F і $F + \Delta F$ відповідно має місце співвідношення:

$$\max_{1 \le j \le N} \left| \sigma_j(F) - \sigma_j(F + \Delta F) \right| \le \left\| \Delta F \right\|_2, \tag{1.8}$$

де $\|\bullet\|_2$ — спектральна матрична норма.

У силу співвідношення (1.8) збурення СНЧ порівнянні зі збуренням даних — ΔF, тобто СНЧ матриці є ***нечутливими до збурних дій***.

Для ВЗ симетричної матриці F має місце аналогічна оцінка:

$$\max_{1 \le j \le n} \left| \lambda_j(F) - \lambda_j(F + \Delta F) \right| \le \left\| \Delta F \right\|_2 \tag{1.9}$$

У силу співвідношення (1.9) збурення ВЗ, як і СНЧ відповідно до (1.8), порівнянні зі збуренням даних — ΔF, ВЗ симетричної матриці є ***нечутливими до збурних дій***, або ***добре обумовленими***.

Чутливість ВВ u_i, який відповідає ВЗ λ_i, в межах матриці F визначається відповідно до співвідношень

$$\sin\theta_i \le \frac{2\|\Delta F\|_2}{gap_{abs}(i,F)} \quad , \tag{1.10}$$

$$\sin\theta_i \le \frac{2\|\Delta F\|_2}{gap_{abs}(i,\overline{F})} \quad , \tag{1.11}$$

де ΔF — збурення матриці F, $\overline{F} = F + \Delta F$, $\overline{u_i}$ — нормований збурений ВВ, θ_i — гострий кут між u_i і $\overline{u_i}$,

$$gap_{abs}(i, F) = \min_{i \neq j} \left| |\lambda_j| - |\lambda_i| \right| \tag{1.12}$$

— ***абсолютна відокремленість*** ВЗ λ_i матриці F.

Твердження. Абсолютна відокремленість ВЗ матриці є мірою чутливості відповідного ВВ до збурних дій.

Аналогічно тому, як це було зроблено у випадку симетричної матриці в співвідношенні (1.12), назвемо ***відокремленістю*** СНЧ σ_i матриці F величину

$$svdgap(i, F) = \min_{i \neq j} |\sigma_j - \sigma_i| .$$

Нехай $F + \Delta F$ — збурена матриця, θ_i — кут між відповідними вхідним і збуреним сингулярними векторами u_i і $\overline{u}_i$, тоді мають місце співвідношення, аналогічні (1.10), (1.11):

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F)} \text{ за умови } svdgap(i,F) \neq 0 ,$$

$$\frac{1}{2}\sin 2\theta_i \le \frac{\|\Delta F\|_2}{svdgap(i,F+\Delta F)} \text{ за умови } svdgap(i,F+\Delta F) \neq 0 .$$

Таким чином, реакція ВВ (СНВ) матриці на збурну дію буде різною, вона буде залежати від значення абсолютної відокремленості (відокремленості) відповідного власного значення (СНЧ): чим більше абсолютна відокремленість (відокремленість) ВЗ (СНЧ), тим менш чутливим до збурних дій буде відповідний ВВ (СНВ).

Питання

1. Що називається власним вектором, власним значенням, власною парою матриці?

2. Скільки власних векторів відповідає кожному власному значенню матриці?
3. Що називається характеристичним многочленом, характеристичним рівнянням матриці?
4. Скільки власних значень має матриця?
5. Що називається спектром матриці?
6. Властивості власних значень і власних векторів матриці. Теорема про спектральне розкладання симетричної матриці.
7. Визначеннння сингулярного розкладання матриці.
8. Що називається сингулярним числом, лівим, правим сингулярним вектором матриці?
9. Як сингулярне розкладання матриці може бути представлено у формі зовнішніх добутків?
10. Чи однозначно визначається сингулярне розкладання матриці?
11. Який вектор називається лексикографічно додатним?
12. Коли сингулярне розкладання називається нормальним? Скільки існує нормальних сигулярних розкладань у матриці?
13. Як пов'язані сингулярне і спектральне розкладання симетричної матриці?
14. Як пов'язані сингулярне і спектральне розкладання матриць A і $A^T A$? Довести.
15. Як пов'язані сингулярне і спектральне розкладання матриць A і AA^T? Довести.
16. Якими (чутливими/нечутливими до збурних дій) є СНЧ матриці? Пояснити.
17. Якими (чутливими/нечутливими до збурних дій) є ВЗ симетричної матриці? Пояснити.
18. Що таке абсолютна відокремленість ВЗ?
19. Показати, що абсолютна відокремленість ВЗ матриці є мірою чутливості відповідного ВВ до збурних дій.
20. Що таке відокремленість СНЧ матриці?

Показати, що відокремленість СНЧ матриці є мірою чутливості відповідного СНВ до збурних дій.

Тема 2. ЗАГАЛЬНА МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ІНФОРМАЦІЙНОГО ПРОЦЕСУ

План

1. Системний комплексний підхід до захисту інформації.
2. Формальне представлення інформаційної системи та її перетворення
3. Зведення формального представлення інформаційної системи до симетричної матриці

1. Системний комплексний підхід до захисту інформації

Процес впровадження нових інформаційних технологій в усі сфери життя суспільства неможливий без розв'язку питань інформаційної безпеки, яка структурується в зовсім різних, але зв'язаних між собою аспектах. Широкомасштабне використання обчислювальної техніки й телекомунікаційних систем, перехід до безпаперової технології, збільшення обсягів оброблюваної інформації й розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даним інформаційних систем (ІС), до їхньої високої вразливості. У сучасних умовах, що вимагають захисту не тільки державної й військової, але й промислової, комерційної, фінансової таємниць, захист інформації в цілому й захист інформації в автоматизованих ІС зокрема стає усе більш складною проблемою, вимагає для свого розв'язку залучення сучасних наукових вишукувань і результатів дослідження.

Теоретичні основи побудови систем захисту інформації дуже складні й, незважаючи на інтенсивність досліджень у цій предметній області, далекі від досконалості.

Розвиток підходів до вирішення проблеми захисту інформації йшов шляхом від забезпечення захисту суто формальними механізмами, що містять головним чином технічні та програмні засоби, через виділення керуючого компонента, ядра безпеки, та розвиток неформальних засобів захисту до формування погляду на захист як на безперервний процес, до розвитку стандартів на захист інформації, посилення тенденції апаратної реалізації функцій захисту, формування висновку про взаємозв'язок захисту інформації, архітектури систем обробки даних та технології їх функціонування, формування *системного комплексного підходу* до захисту інформації.

Під *системністю* в даний час розуміється пояснювальний принцип наукового пізнання, що вимагає досліджувати явища в їх залежності від внутрішньо пов'язаного цілого, яке вони утворюють, набуваючи завдяки цьому нові властивості. Використання цього основоположного принципу теорії захисту інформації дає можливість для наукового обгрунтування структуризації процесів захисту, враховуючи їх взаємозв'язок і взаємовплив.

Методологічні принципи й теоретичні положення системного підходу дають змогу:

- розглядати об’єкт дослідження як цілісну систему, відносно відокремлену від зовнішнього середовища і водночас пов’язану з ним, тобто вивчати цей об’єкт у тісному зв’язку й взаємодії з іншими об’єктами;
- відстежувати зміни, що відбуваються в системі внаслідок зміни окремих її ланок;
- вивчати специфічні системні якості;

- доходити обґрунтованих висновків щодо закономірностей розвитку системи;
- визначати оптимальний режим її функціонування.

Основні етапи реалізації системного підходу:

- формування проблеми;
- виокремлення цілі або сукупності цілей;
- визначення альтернативних засобів, за допомогою яких можна досягти поставлених цілей;
- визначення ресурсів, необхідних при використанні кожної системи;
- побудова математичної моделі, тобто формалізованих залежностей між цілями та альтернативними засобами їх досягнення;
- визначення критеріїв вибору найкращої альтернативи.

Основні принципи системного підходу:

- принцип системності, або єдності — розгляд і вивчення об'єктів дослідження як цілісних систем. Передбачає розгляд системи, з одного боку, як цілого, а з другого — сукупності компонентів (елементів, підсистем, системотвірних відношень);
- принцип кінцевої мети — зведення до абсолютного пріоритету кінцевої або глобальної мети (основної функції, основного призначення тощо);
- принцип зв'язності — кожний компонент системи розглядається разом із його зв'язками з оточенням;
- принцип модульності — здебільшого в системі є сенс реалізувати декомпозицію на складові різного ступеня загальності, розглядаючи її як сукупність певних модулів і зв'язків між ними;
- принцип ієрархічності пізнання — найчастіше в системі доцільно реалізувати ієрархічну побудову і/або впорядкувати її складові за важливістю. Принцип вимагає трирівневого вивчення об'єкта: рівень 1 — вивчення самого об'єкта («власний» рівень); рівень 2 — вивчення цього об'єкта як елемента більш складної системи («зовнішній» рівень); рівень 3 — вивчення цього об'єкта відповідно до його складових («нижчий» рівень);
- принцип функціональності — спільний розгляд структури і функцій об'єкта з огляду на пріоритет функцій над структурою. На практиці принцип функціональності означає, зокрема, що в разі надання системі нових функцій корисно переглянути її структуру, а не намагатися реалізувати нову функцію в старій схемі реалізації системи;
- принцип розвитку — має закладатися при побудові штучних систем як здатність до вдосконалення, розвитку системи за умови збереження якісних особливостей. Межі розширення функцій і модернізації повинні передусім чітко усвідомити творці штучної системи, оскільки існують доцільні межі її універсальності. Можливості для розвитку закладаються через надання системі властивостей до самонавчання, самоорганізації, штучного інтелекту;
- принцип децентралізації — в управлінні системою співвідношення між централізацією та децентралізацією визначається призначенням та метою системи. При цьому ступінь централізації має бути мінімальний, що забезпечить досягнення остаточної мети;
- принцип невизначеності — дуже часто ми працюємо з системою, про яку далеко не все знаємо й не все розуміємо в її поведінці. Тому невизначеності та випадковості доводиться брати до уваги при визначенні стратегії і тактики розвитку системи;
- принцип формалізації — системний підхід має на меті здобуття кількісних характеристик, створення методів, що звужують неоднозначність понять, визначень, оцінок тощо;
- принцип інтеграції — спрямованість системного підходу на вивчення інтегративних властивостей і закономірностей системи, розкриття базисних механізмів формування єдиного цілого.

І хоча системність проголошена, але на практиці реалізувати це в галузі інформаційної безпеки завдяки складності системи захисту інформації не так просто. Наприклад, лише зараз тільки починають розроблятися крипто-

стеганографічні системи, що засновані на врахуванні необхідного взаємозв'язку між криптографічною та стеганографічною складовими системи, а до цього моменту вони розглядалися окремо.

Під *комплексністю* системи захисту інформації розуміється поєднання наступних заходів:

1. Законодавчі заходи. Використання законодавчих актів, що регламентують права та обов'язки фізичних та юридичних осіб, а також держави у галузі захисту інформації;
2. Морально-етичні заходи. Створення та підтримка на об'єкті такої моральної атмосфери, у якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників різко негативно;
3. Фізичні заходи. Створення фізичних перешкод для доступу сторонніх осіб до інформації, що охороняється;
4. Адміністративні заходи. Організація відповідного режиму секретності, пропускного та внутрішнього режиму;
5. Технічні заходи. Застосування електронних та інших пристроїв для захисту інформації;
6. Криптографічні заходи. Застосування шифрування та кодування для приховання оброблюваної та переданої інформації від несанкціонованого доступу;
7. Програмні заходи. Застосування програмних засобів розмежування доступу.

Комплексність може бути досягнута лише за взаємоузгодженої участі у вирішенні відповідних завдань професійних фахівців із захисту інформації, керівників, фахівців, які задіяні у процесах збирання, передачі, зберігання, обробки та використання інформації, а ефективне вирішення проблем захисту інформації. можливо лише за наявності розвиненого та адекватного *наукового базису*.

Напрацьований в області інформаційної безпеки математичний апарат, що включає в якості інструментів теорію ймовірностей, дискретну математику, теорію нечітких множин, нечітку логіку, штучні нейронні мережі і т.д., виявився недостатнім для опису об'єктів, які погано формалізуються, мають властивості, погано відомі апріорі й мінливі в процесі функціонування, якою є будь-яка ІС.

З кінця минулого століття отримав розвиток некласичний підхід при моделюванні та дослідженні СЗІ, заснований на аналогіях архітектури і цілей функціонування складних технічних і біологічних систем, що є природними системами управління. Основна ідея полягає в наступному: проблему забезпечення безпеки складних автоматизованих та телекомунікаційних систем необхідно вирішувати комплексно, орієнтуючись на організацію біологічних систем, які мають високу захищеність. Ієрархічний принцип організації властивий як біологічним, так і складним технічним системам.

Поняття ієрархії. Не строго: ієрархія - це порядок підпорядкованості нижчих ланок вищим, на які розбивається деяка множина. Ієрархічна організація - структура з вертикальною формою управління; піраміда, кожним рівнем якої керує вищий рівень. Визначимо строго поняття ієрархії.

Нехай "≤" — бінарне відношення нестрогого порядку на деякій множині S (антисиметричне, транзитивне, рефлексивне). Для будь-якого відношення $x \le y,\ x, y \in S$, можна визначити відношення $x < y$, що означає $x \le y, x \ne y$. Кажуть, що y покриває x, якщо $x < y$ і не існує такого $t \in S$, що $x < t < y$.

Визначення. Нехай X — скінченна частково впорядкована множина з найбільшим елементом $\bar{x}$. Множина X є ієрархією, якщо існує така розбивка X на підмножини $L_k,\ k = \overline{1,h}$, де $L_1 = \{\bar{x}\}$, що виконуються наступні умови:

1) $\left(x \in L_k\right) \Rightarrow \left(x^- \subset L_{k+1},\ k = \overline{1,h-1}\right)$, де $x^- = \{\, y \,|\, x \text{ покриває } y \,\}$;

2) $\left(x \in L_k\right) \Rightarrow \left(x^+ \subset L_{k-1},\ k = \overline{2,h}\right)$, де $x^+ = \{\, y \,|\, y \text{ покриває } x \,\}$.

Для кожного $x \in X$ існує вагова функція, сутність якої залежить від явища, для якого будується ієрархія: $w_x : x^- \to [0,1],\ \sum_{y \in x^-} w_x(y) = 1$. Множини L_k називаються рівнями ієрархії, w_x — функція пріоритету відносно елемента x.

Крім того, обом видам систем властива спільність цілей: підтримка життєздатності складної системи протягом тривалого часу за рахунок забезпечення надійного кодування, зберігання, перетворення та передачі інформації. Надання технічним системам позитивних якостей біосистем, які відповідають за безпеку та надійність інформаційних процесів, змінює сам підхід до створення складних комп'ютерних систем. Такий підхід найчастіше орієнтований насамперед на нейромережну елементну базу, оскільки штучні нейронні мережі найбільш подібні до біосистем і мають необхідну сукупність властивостей, серед яких здатність до узагальнення, адаптації, самонавчання і т.д., але не тільки.

Новим і надзвичайно перспективним є підхід до проблеми аналізу стану й створення систем захисту інформації, заснований на теорії збурень і матричному аналізі, який дає можливість для визначення чутливості довільного об'єкта до змін вхідних даних, ступеня залежності стану об'єкта від збурних дій для апріорної оцінки властивостей об'єкта.

2. Формальне представлення інформаційної системи та її перетворення

Будь-який інформаційний процес (ІП) визначається зміною параметрів, що його задають, або приведенням одних параметрів (вихідних) у відповідність з іншими (вхідними) за деяким законом. При формальному представленні досліджуваного процесу у вигляді його математичної моделі виділяється лише скінченна кількість параметрів (вхідних і вихідних), що несуть у собі найціннішу інформацію про його основні закономірності. Таким чином, будь-який ІП у найзагальнішому вигляді можна формально подати як неперервну вектор-функцію скінченної кількості змінних, значенням якої є вектор скінченного розміру:

$$\Phi(x_1,\ldots,x_n) = \begin{pmatrix} \varphi_1(x_1,\ldots,x_n) \\ \varphi_2(x_1,\ldots,x_n) \\ \vdots \\ \varphi_m(x_1,\ldots,x_n) \end{pmatrix} = \begin{pmatrix} \Phi_1 \\ \Phi_2 \\ \vdots \\ \Phi_m \end{pmatrix}, \qquad (2.1)$$

$$\Phi : D(\Phi) \to R^m,\ D(\Phi) \subseteq R^n,$$

що є законом відповідності вихідних параметрів (значення функції) $(\Phi_1,\Phi_2,...,\Phi_m)\in R^m$ вхідним (аргументам) $(x_1,...,x_n)\in D(\Phi)\subseteq R^n$, де $D(\Phi)$ — область визначення $\Phi(x_1,...,x_n)$. Співвідношення (2.1) — це загальне представлення будь-якого ІП. Кожна конкретна математична модель ІП задається лише певним видом функції (2.1).

Будь-яка вектор-функция (2.1) породжує m дійсних функцій

$$\varphi_i : D(\Phi)\to R,\ i=\overline{1,m}, \qquad (2.2)$$

на своїй області визначення $D(\Phi)$. Таким чином: довільний неперервний ІП (або інформаційна система (ІС), що розглядається як результат процесу її синтезу) може бути формально представлений у вигляді скінченної множини дійсних функцій (2.2) скінченної кількості змінних, а аналіз цього процесу зведений до аналізу отриманих функцій.

При побудові такої функції (2.1) для реального процесу (системи) отримання реальних значень для вхідних параметрів, що є результатами вимірювань, експериментів і т.д., передбачає дискретність цих значень. Крім того, процес обробки функції (2.1) з використанням обчислювальних засобів та чисельних методів так чи інакше призведе до її дискретизації, в результаті якої вийде n-вимірна матриця з елементами з простору R^m. Оскільки будь-яка вектор-функція, що діє в простор R^m, породжує m дійсних функцій (2.2) на своїй області визначення, то результат дискретизації може бути представлений як множина, що складається з m n-вимірних матриць $M_1,M_2,...,M_m$ з елементами з простору R, кожна з яких відповідає своїй певній функції (2.2). Таким чином: довільний ІП (чи ІС, що розглядається як результат процессу її синтеза) може бути формально представлений в вигляді скінченної множини матриць $M_1,M_2,...,M_m$ певної скінченної вимірності з дійсними елементами, а тому аналіз будь-якого ІП принципово можна звести до аналізу відповідних матриць.

Вихідні параметри $\Phi_1,\Phi_2,...,\Phi_m$ можуть виявитися залежними один від іншого, тоді отримувані m n-вимірних матриць $M_1,M_2,...,M_m$ також виявляться залежними. Однак на процесі аналізу стану ІС це ніяк не відіб’ється, оскільки цей процес не змінює наявні залежності між вхідними та вихідними параметрами.

Як показує практика, з урахуванням зручності обробки одержуваної моделі, найчастіше при моделюванні реальних процесів і об'єктів використовуються двовимірні матриці, які в силу наведеного нижче зауваження і розглядатимуться далі при описі ІС.

Зауваження. Якщо в отриманій при моделюванні ІП (ІС) сукупності $M_1,M_2,...,M_m$ матриць $n>2$, то довільній M_j, $j=\overline{1,m}$, можна поставити у відповідність скінченну множину матриць вимірності 2, кожна з яких отримується з M_j шляхом фіксування у ній всіх індексів, крім двох.

Твердження. Будь-який ІП (ІС) може бути формально представлений у вигляді скінченної множини двовимірних дійсних матриць, а тому формальний *аналіз процесу принципово можна звести до аналізу двовимірних матриць*.

Для спрощення викладу, не обмежуючи при цьому спільності міркувань, у якості математичної моделі ІС будемо розглядати двовимірну (прямокутну або квадратну) матрицю F.

Результат будь-яких дій над ІС, що моделюється, у загальному випадку можна представити як збурення ΔF матриці F, самі дії — збурні дії на F, а завдання будь-якого перетворення системи, тобто генерації нової, для якої стара є вхідними даними, - це завдання одержання збуреної матриці для вхідної матриці F, до того ж результуюча матриця очевидно задовольняє співвідношенню:

$$\overline{F} = F + \Delta F, \qquad (2.3)$$

де $\Delta F = f(F)$, тобто ΔF є деякою функцією матриці F.

Таким чином, зі співвідношення (2.3) випливає наступне

Твердження. Будь-які перетворення довільної ІС можуть бути формально представлені у вигляді елементарних матричних операцій.

Таким чином, у якості набору формальних параметрів, що однозначно визначають й всебічно характеризують будь-яку ІС, можна використовувати кожний з наборів, який однозначно визначає довільну двовимірну матрицю. Назвемо такі набори параметрів *повними*.

Розглянемо один з можливих повних наборів параметрів. Враховуючи, що для матриці F однозначно визначаються елементи її нормального сингулярного розкладання — сингулярні числа, ліві і праві сингулярні вектори, то совокупність цих параметрів може розглядатися як повний набір для ІС.

Будь-яке перетворення ІС збурить її матрицю F, а значить певним чином збурить її СНЧ і СНВ. Тому має місце наступне

Твердження. Будь-яке перетворення ІС може бути формально представленим у вигляді сукупності збурень СНЧ і (або) СНВ її матриці, що дозволяє природно звести задачу аналізу процесу перетворення й підсумкового стану системи до аналізу збурень СНЧ і СНВ, а задачу синтезу системи із заданими властивостями - до задачі забезпечення певних характеристик збурень СНЧ і СНВ її матриці. ***Це твердження є основою загального підходу до аналізу стану систем захисту інформації (ЗПАІС), заснованому на теорії збурень та матричному аналізі.***

Таким чином, про результат перетворення ІС, її властивості, у тому числі й про одну з найбільш важливих властивостей - чутливість, можна судити по характерних рисах сукупності збурень однозначно визначальних її параметрів - СНЧ і СНВ. При цьому чутливістю ІС назвемо чутливість задачі її формування. Як зазначалося в матеріалах Теми 1, СНЧ $\sigma_j(F)$, $\sigma_j(F+\Delta F)$, $j=\overline{1,n}$, матриць F і $F+\Delta F$ відповідно є нечутливими до збурних дій, чи добре обумовленими, а от реакція СНВ матриці на збурну дію буде різною навіть у межах однієї матриці, вона буде залежати від значення відокремленості відповідного СНЧ: чим більше відокремленість СНЧ, тим менш чутливим до збурних дій буде відповідний СНВ.

Оскільки СНЧ є добре обумовленими, їх збурення порівнянні зі збуренням даних — ΔF, тобто СНЧ матриці є нечутливими до збурних дій незалежно від того, чутливою або нечутливою виявиться розглянута задача по формуванню $F + \Delta F$, тобто задача перетворення ІС.

Зауваження. Для оцінки чутливості задачі перетворення ІС із матрицею F має сенс аналізувати лише збурення СНВ F, що відбулися в результаті перетворення.

Результат перетворення системи для встановлення міри чутливості до збурних дій будемо розглядати у вигляді сукупності збурень СНВ її матриці.

Твердження. Чутливість задачі, що полягає в довільному перетворенні ІС, математичною моделлю якої є двовимірна матриця, буде визначатися чутливістю збурених перетворенням системи СНВ матриці.

Розглянемо другий можливий повний набір параметрів. Якщо F — симетрична $n \times n$-матриця, то в якості повного набору формальних параметрів для неї можна розглядати сукупність власних значень і власних векторів, отриманих за допомогою нормального спектрального розкладання.

Для ІС, моделлю якої є симетрична матриця, має місце твердження:

Твердження. Будь-яке перетворення ІС у випадку симетричності її матриці представляється у вигляді збурень спектра й (або) ВВ матриці, що однозначно визначаються нормальним СР, що дозволяє звести задачу аналізу процесу перетворення й підсумкового стану ІС до аналізу збурень ВЗ і ВВ, а задачу синтезу системи із заданими властивостями - до забезпечення певних характеристик збурень ВЗ і ВВ її матриці.

ВЗ симетричної матриці є добре обумовленими, тобто нечутливими до збурних дій, чого не можна стверджувати в загальному випадку для несиметричних матриць. Для власних векторів мірою чутливості до збурних дій є абсолютна відокремленість ВЗ матриці.

Твердження. Чутливість задачі, що полягає в довільному перетворенні ІС, математичною моделлю якої є симетрична матриця, буде визначатися чутливістю збурених перетворенням системи ВВ її матриці.

Збурення ВЗ (як і СНЧ) порівнянні зі збуренням даних — ΔF, ВЗ симетричної матриці є нечутливими до збурних дій незалежно від того, чутливою чи нечутливою виявиться розглянута задача по формуванню $F + \Delta F$.

Зауваження. Для оцінки чутливості задачі перетворення ІС із симетричною матрицею F має сенс аналізувати лише збурення ВВ F, що відбулися в результаті перетворення. Результат перетворення ІС для встановлення міри її чутливості до збурних дій будемо розглядати у вигляді сукупності збурень ВВ відповідної матриці.

Спираючись на зв'язок між сингулярним і спектральним розкладаннями відповідних матриць, можна перетворити алгоритми розв'язку симетричної проблеми ВЗ в алгоритми обчислення сингулярного розкладання. Це перетворення виконується не прямолінійно, оскільки сингулярне розкладання має додаткову структуру, яка часто може бути використана для підвищення ефективності й точності алгоритмів.

Для $n=3$ геометричне представлення довільного перетворення ІС у випадку рішення задачі чутливості подане на рис.2.1, де u_1, u_2, u_3 — СНВ (ВВ) матриці поданої системи, $\bar{u}_1, \bar{u}_2, \bar{u}_3$ — СНВ (ВВ) матриці збуреної ІС.

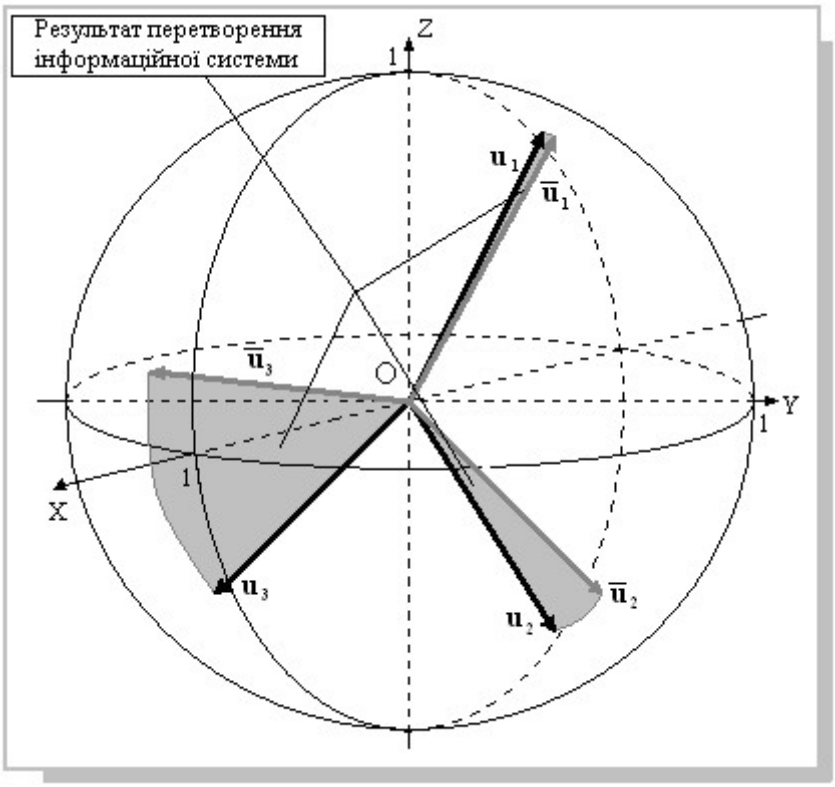


Рис.2.1. Геометричне представлення довільного перетворення інформаційної системи

3. Зведення формального представлення інформаційної системи до симетричної матриці

Нехай матриця F симетрична. Тоді в якості визначального її повного набору параметрів можна використовувати, як показано вище, як множину СНЧ і СНВ, так і спектр матриці й множину ВВ спеціального виду. Перевагу в цьому випадку слід віддати другому набору параметрів у силу наступних зауважень:

- побудова СР симетричної матриці має ряд переваг в обчислювальному сенсі в порівнянні з побудовою сингулярного розкладання для матриці довільної структури того ж розміру й того ж рівня заповнення;
- при цьому ВЗ симетричної матриці, як і її сингулярні числа, є добре обумовленими відповідно до (1.9), а ВВ, як і СНВ можуть бути в межах одної матриці як добре, так і погано обумовленими, що залежить від відокремленості відповідних ВЗ (СНЧ).

Однак, як правило, на практиці матриця ІС не задовольняє властивості: $F = F^T$. Поставимо у відповідність довільній F дві симетричні матриці $A,\ B$ того ж розміру за наступним правилом:

$$F=\begin{pmatrix} a_{11}\,a_{12}\;a_{13}\ldots a_{1n} \\ a_{21}\,a_{22}\;a_{23}\ldots a_{2n} \\ a_{31}\,a_{32}\;a_{33}\ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}\,a_{n2}\;a_{n3}\ldots a_{nn} \end{pmatrix} \rightarrow A=\begin{pmatrix} a_{11}\,a_{12}\,a_{13}\ldots a_{1n} \\ a_{12}\,a_{22}\,a_{23}\ldots a_{2n} \\ a_{13}\,a_{23}\,a_{33}\ldots a_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}\,a_{2n}\,a_{3n}\ldots a_{nn} \end{pmatrix}, B=\begin{pmatrix} a_{11}\,a_{21}\,a_{31}\ldots a_{n1} \\ a_{21}\,a_{22}\,a_{32}\ldots a_{n2} \\ a_{31}\,a_{32}\,a_{33}\ldots a_{n3} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}\,a_{n2}\,a_{n3}\ldots a_{nn} \end{pmatrix}, \qquad (2.4)$$

які будемо розглядати як симетричні матриці ІС. Це ніяк не обмежує міркувань у силу наступного. Нехай ΔF — матриця довільного збурення, яке зазнає F (або $\overline{F}$). В загальному випадку $\Delta F \neq \Delta F^T$. Матриці ΔF поставимо в співвідношення дві симетричні матриці того ж розміру, використовуючи правило (2.4), розглядаючи матрицю, що відповідає верхньому (нижньому) трикутнику ΔF як матрицю збурення для F ($\overline{F}$), яка отримана на основі $A(B)$, що дає принципову можливість матрицю довільного збурення й, як наслідок, матрицю $\overline{F}$ також розглядати як симетричні.

Будь-які збурення матриці F представляються в вигляді збурень верхнього (нижнього) трикутника матриці $A(B)$ з наступним симетричним відображенням результату відносно головної діагоналі $A(B)$. Нехай підсумком такого збурення є симетричні матриці $\overline{A}$ і $\overline{B}$. При остаточному формуванні матриці $\overline{F}$ використовується верхній трикутник $\overline{A}$ і нижній трикутник матриці $\overline{B}$.

Питання

1. В чому полягають труднощі при створенні теоретичного базису побудови систем захисту інформації?
2. Що таке чутливість інформаційної системи?
3. Формальне представлення інформаційної системи та її перетворення.
4. Пояснити, чому будь-які перетворення інформаційної системи, зокрема системи захисту інформації, можна представити у вигляді елементарних матричних операцій.
5. Що таке сингулярне розкладання матриці? Коли сингулярне розкладання визначається однозначно?
6. Збурення яких формальних параметрів ситеми має сенс аналізувати для оцінки її чутливості до збурних дій? Чому?
7. Чим визначається чутливість задачі, яка полягає в довільному перетворенні інформаційної ситеми? Пояснити.
8. Обумовленість сингулярних чисел (власних значень) , сингулярних векторів (власних векторів) матриці.
9. Як повязані сингулярне і спектральне розкладання симетричної матриці?
10. Геометричне представлення довільного перетворення інформаційної системи.
11. Яким чином відбувається зведення формального представлення інформаційної системи до симетричної матриці? Які переваги дає симетричний вигляд матриці інформаційної системи?

Тема 3. ЦИФРОВА СТЕГАНОГРАФІЯ

План

1. Цифрова стеганографія. Предмет, термінологія, області застосування.
2. Узагальнена структурна схема стеганосистеми.
3. Класифікація контейнерів.
4. Атаки на стеганосистеми
5. Пропускна спроможність каналів передачі прихованої інформації
6. Поняття стійкості стеганосистеми
7. Локалізація області збурень параметрів стеганоповідомлення для забезпечення певних властивостей стеганосистеми
   7.1. Забезпечення надійності сприйняття стеганоповідомлення
   7.2. Чутливість стеганоповідомлення до збурних дій

1. Цифрова стеганографія. Предмет, термінологія, області застосування

Завдання захисту інформації від несанкціонованого доступу вирішувалося за всіх часів протягом історії людства. Уже в прадавньому світі виділилося два основні напрямки розв'язку цього завдання, що існують і по сьогоднішній день: криптографія й стеганографія. Метою криптографії є приховання вмісту повідомлень за рахунок їх шифрування. На відміну від цього, при стеганографії приховується сам факт існування таємного повідомлення.

Слово «стеганографія» має грецьке коріння й буквально означає «тайнопис». Історично цей напрямок з'явився першим, але потім був витиснений криптографією. Тайнопис здійснюється всілякими способами. Загальною рисою цих способів є те, що приховуване повідомлення або додаткова інформація (ДІ) вбудовується в деякий об'єкт, що не привертає увагу, який далі називається ***контейнером***. Результат такого вбудовування будемо називати ***стеганоповідомленням*** (СП), а сам процес вбудовування - ***стеганоперетворенням*** (СПр) контейнера. Потім стеганоповідомлення відкрито транспортується адресатові або зберігається в отриманому виді.

При використанні криптографії наявність шифрованого повідомлення сама по собі привертає увагу супротивників, при використанні стеганографії ж наявність прихованого зв'язку залишається непомітною.

Згідно із ***принципом Кергоффа***, система захисту інформації (зокрема стеганосистема) повинна забезпечувати свої функції навіть при повній поінформованості супротивника про її структуру й алгоритмах функціонування; Уся таємність системи захисту переданих відомостей повинна полягати в ключі, тобто в попередньо (як правило) розділеному між адресатами фрагменті інформації.

Стеганографія - це наука, яка вивчає способи й методи приховування конфіденційної/секретної інформації, основною задачею якої є приховування самого факту існування секретних даних при їхній передачі, зберіганні або обробці. Під приховання існування інформації мається на увазі не тільки неможливість виявлення в перехопленому повідомленні наявності іншого (прихованого) повідомлення, але й взагалі неможливість виникнення будь-яких підозр на цей рахунок. Слово «непомітність» для вбудованої ДІ має на увазі

обов'язкове включення людини в систему стеганографічної передачі даних. Людина тут може розглядатися як додатковий приймач даних, що пред'являє до системи передачі вимоги, що досить важко формалізувати.

Розвиток засобів обчислювальної техніки дав новий поштовх для розвитку *комп'ютерної стеганографії*. З'явилося багато нових областей застосування. Повідомлення вбудовують тепер у цифрові дані, які, як правило, мають аналогову природу. Це - аудіо, зображення, відео. Відомі також пропозиції по вбудовуванню інформації в текстові файли й в файли програм.

Розвиток стеганографії сьогодні відбувається стрімко й багатогранно. Можна виділити дві причини популярності досліджень в області стеганографії в цей час: обмеження на використання криптозасобів у ряді країн світу (у тому числі, в Україні) і поява проблеми захисту прав власності на інформацію, представлену в цифровому виді. Перша причина спричинила велику кількість досліджень у дусі класичної стеганографії (тобто приховування факту передачі інформації), друга - ще більш численні роботи в області так званих водяних знаків. *Цифровий водяний знак* (ЦВЗ) – спеціальна мітка, впроваджувана в зображення або інший цифровий сигнал з метою тим або іншим способом контролювати його використання.

Для конкретності далі будемо розглядати цифрові зображення (ЦЗ).

Можна запропонувати наступну класифікацію напрямків, які містить у собі стеганографія:

- вбудовування інформації з метою її прихованої передачі (класична стеганографія);
- вбудовування цифрових водяних знаків (watermarking);
- вбудовування ідентифікаційних номерів (fingerprinting) - «відбитків пальців»;
- вбудовування заголовків (captioning).

Класична стеганографія зазвичай спрямована на організацію *прихованого каналу зв'язку* в каналі загального користування й до недавнього часу залучала до себе основну увагу фахівців. Однак на сьогоднішній день у зв'язку з бурхливим розвитком інформаційних технологій, комп'ютерної техніки, використовуваної повсюдно, переводу левиної частки інформації в цифрову форму акценти трохи змістилися, принаймні, як можна судити по публікаціях у відкритій пресі: основна увага приділяється другому з перерахованих напрямків стеганографії (тобто ЦВЗ).

ЦВЗ можуть застосовуватися, в основному, для захисту від копіювання й несанкціонованого використання. У зв'язку з розвитком технологій мультимедіа гостро встало питання захисту авторських прав і інтелектуальної власності, представленої в цифровому виді. Прикладами можуть бути фото, аудіо й відеозаписи й т.д. Переваги, які дають представлення й передача повідомлень у цифровому виді, можуть виявитися перекресленими легкістю, з якої можливо їх злодійство або модифікація. Тому розробляються різні заходи захисту інформації, організаційного й технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації й полягає у вбудовуванні в об'єкт, що захищається, невидимих (видимих) міток - ЦВЗ. Розробки в цій області ведуть в усьому світі. Оскільки методи ЦВЗ почали

розроблятися зовсім недавно (першою статтею на цю тему була, очевидно, робота 1989 р.), то тут є багато неясних проблем, що вимагають свого рішення. Назву ці методи отримали від усім відомого способу захисту цінних паперів, у тому числі й грошей, від підробки. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їхню коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника, або яку-небудь керуючу інформацію. Найбільш підходящими об'єктами захисту за допомогою ЦВЗ є нерухомі зображення, файли аудіо й відеоданих.

Технологія вбудовування *ідентифікаційних номерів* виробників має багато спільного з технологією ЦВЗ. Відмінність полягає в тому, що при вбудовуванні ідентифікаційних номерів кожна захищена копія має свій унікальний номер, що вбудовується (звідси й назва - дослівно «відбитки пальців»). Цей ідентифікаційний номер дозволяє виробникові відслідковувати подальшу долю свого дітища: чи не зайнявся хто-небудь із покупців незаконним тиражуванням. Якщо так, то «відбитки пальців» швидко вкажуть на винного.

Вбудовування заголовків (невидиме) може застосовуватися, наприклад, для підпису медичних знімків, нанесення легенди на карту й т.д. Метою є зберігання різнорідно представленої інформації в єдиному цілому. Це, мабуть, єдине застосування стеганографії, де в явному виді відсутній потенційний порушник.

2. Узагальнена структурна схема стеганосистеми

Завдання вбудовування й виділення повідомлень із іншої інформації виконує стеганосистема, яка, як правило, складається з наступних основних елементів, представлених на рис.3.1:

- попередній кодер - пристрій, призначене для перетворення приховуваного повідомлення (конфіденційної/секретної інформації (КІ), ЦВЗ) до виду, зручного для вбудовування в контейнер;
- кодер - пристрій, призначене для здійснення вкладення додаткової інформації в контейнер з урахуванням його моделі (його особливостей);
- пристрій виділення вбудованого повідомлення;
- детектор – пристрій, призначений для визначення наявності вкладеної ДІ;
- декодер – пристрій, що відновлює конфіденційну/секретну інформацію. Цей вузол може бути відсутнім.

Дані, що містять приховане повідомлення, можуть піддаватися навмисним атакам або випадковим перешкодам, зокрема, у каналі атаки.

Перш, ніж здійснити вкладення КІ, ЦВЗ у контейнер, КІ (ЦВЗ) повинна бути перетворена до деякого підходящого виду, наприклад, якщо в якості контейнера виступає зображення, то й перетворена в попередньому кодері КІ (ЦВЗ) найчастіше представляється як (двовимірний) масив біт. Обробка в попередньому кодері виконується з використанням ключа *K* для забезпечення таємності вбудовування. Результатом попереднього кодування є додаткова інформація, що представляє із себе, як правило (але не обов'язково), бітову послідовність. Далі ДІ «вбудовується» у контейнер, наприклад, шляхом модифікації молодших значущих біт значень яскравості пікселів (у випадку цифрового зображення-контейнера). Цей процес можливий завдяки особливостям системи сприйняття людини: добре відомо, що зображення

мають велику психовізуальну надлишковість; око людини подібне низькочастотному фільтру, що пропускає дрібні деталі. Особливо непомітні спотворення у високочастотній області зображень. Ці особливості людського зору використовуються, наприклад, при розробці алгоритмів стиску зображень і відео.

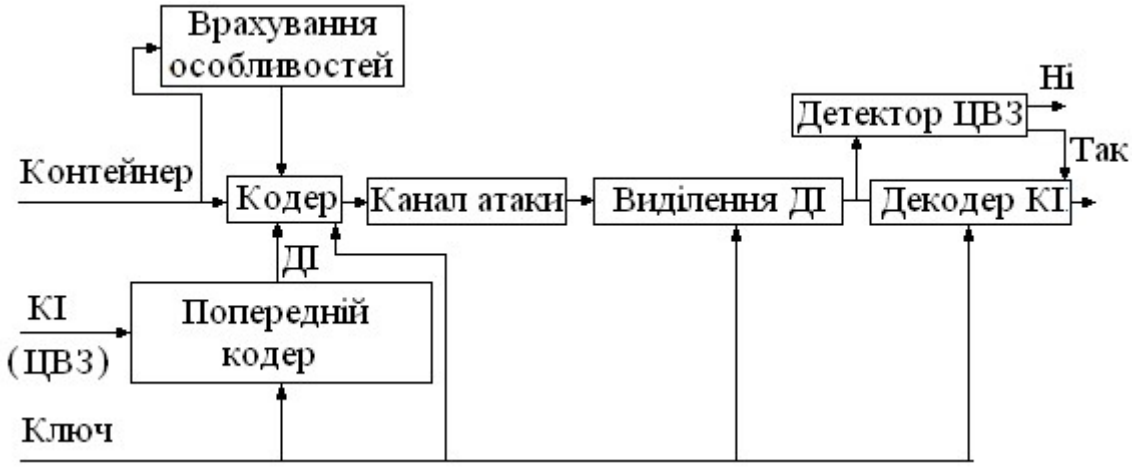


Рис. 3.1. Схема типової стеганосистеми

Процес вбудови ДІ також повинен ураховувати властивості системи сприйняття людини. Стеганографія використовує наявну в сигналах психовізуальну надлишковість, але іншим, чим при стиску даних, образом. Наведемо простий приклад. Розглянемо півтонове зображення з 256 градаціями сірого. Добре відомо, що око людини не здатне помітити зміну молодшого значущого біта. Ще в 1989 році був отриманий патент на спосіб прихованого вкладення інформації в зображення шляхом модифікації молодшого значущого біта. У цьому випадку детектор стего аналізує тільки значення цього біта для кожного пікселя, а око людини, навпаки, сприймає тільки старші 7 біт. Хоча даний метод простий у реалізації й ефективний, він не задовольняє деяким важливим вимогам, зокрема не забезпечує стійкість до атак проти вбудованого повідомлення.

У стегодетекторі відбувається виявлення ДІ в можливо зміненому зображенні. Ця зміна може бути обумовлена впливом помилок у каналі зв'язку, операцій обробки сигналу, навмисних атак порушників.

3. Класифікація контейнерів

Розрізняють два основні типи контейнерів: ***потоковий*** і ***фіксований***.

Потоковий контейнер являє собою послідовність біт, що безперервно подається; повідомлення вкладається в нього в реальному масштабі часу, так що в кодері невідомо заздалегідь, чи вистачить розмірів контейнера для передачі всього повідомлення. В один контейнер великого розміру може бути вбудовано й кілька повідомлень. Потоковий контейнер має велике практичне значення: наприклад, стегоприставка до звичайного телефону: під прикриттям звичайного, незначного телефонного переговору можна передавати іншу розмову, дані й інше, і, не знаючи секретного ключа, не можна не тільки довідатися про зміст прихованої передачі, але й сам факт її існування. Не випадково, що робіт, присвячених розробці стеганосистем з потоковим контейнером практично не зустрічається у відкритій пресі.

У ***фіксованого*** контейнера розміри й характеристики заздалегідь відомі, що дозволяє здійснювати вкладення даних оптимальним у деякому сенсі образом.

Контейнер може бути ***обраним, випадковим*** або ***нав'язаним***. ***Обраний контейнер*** залежить від повідомлення, що вбудовується, а в граничному випадку є його функцією. Цей тип контейнера більше характерний для класичної стеганографії. ***Нав'язаний контейнер*** може з'явитися в сценарії, коли особа, що надає контейнер, підозрює про можливу приховану переписку й бажає запобігти її. На практиці ж найчастіше зустрічаються з ***випадковим контейнером***.

Вбудовування повідомлення в контейнер проводиться з використанням ключа, одного або декількох. Приховувана інформація, як правило, вбудовується відповідно до ключа в ті відліки, спотворення яких не приводить до істотних спотворень контейнера. Ці відліки утворюють ***стеганошлях***. Залежно від області застосування під істотним спотворенням можна розуміти спотворення, що приводить як до неприйнятності для людини-адресата заповненого контейнера, так і до можливості виявлення факту наявності прихованого повідомлення після стеганоаналізу.

Захист цифрового контейнера від його несанкціонованого використання доцільно проводити з використанням ЦВЗ, які можуть бути трьох типів: ***робастні, хрупкі й напівхрупкі*** (semifragile), і використовуються залежно від переслідуваної мети.

Під робастністю ЦВЗ розуміється його стійкість до різного роду збурних дій на СП. Більшість досліджень у цьому напрямку стеганографії присвячено робастним ЦВЗ.

Хрупкі ЦВЗ руйнуються при незначній модифікації СП; вони застосовуються для автентифікації контейнера. Відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ все ж таки допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, тому що законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність від засобів електронного цифрового підпису полягає в тому, що хрупкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни, що робить їх кращими в умовах автентифікації контейнера.

Напівхрупкі ЦВЗ стійкі стосовно одних збурних дій і нестійкі стосовно інших. Загалом кажучи, усі ЦВЗ можуть бути віднесені до цього типу. Однак напівхрупкі ЦВЗ спеціально проектують так, щоб бути нестійкими стосовно певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиск зображення, але забороняти вирізку з нього або вставку в нього фрагмента.

4. Атаки на стеганосистеми

Стеганосистема утворює стеганоканал, по якому передається СП. Цей канал вважається підданим впливам з боку порушників. Можна виділити три типи порушників, яким повинна протистояти стегосистема: ***пасивний, активний і злочинний порушники***.

1. ***Пасивний порушник*** може лише виявити факт наявності стегоканала й (можливо) читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежить від стійкості системи шифрування, і це

питання, як правило, не розглядається в стеганографії. Якщо в порушника є можливість виявити факт наявності прихованого каналу передачі повідомлень, то стеганосистема зазвичай вважається нестійкою. Хоча існують і інші точки зору на стійкість стегосистем. Здійснення виявлення стеганоканалу є найбільш трудомістким завданням, а захист від виявлення вважається основним завданням стеганографії за визначенням.

2. Діапазон дій ***активного*** порушника значно ширше. Приховане повідомлення може бути їм вилучене або зруйноване. У цьому випадку адресат, можливо, довідається про факт втручання. У більшості випадків це суперечить інтересам порушника (наприклад, за юридичними мотивами). Інша справа - видалення або руйнування цифрового водяного знака, які можуть розглядатися як основні погрози в цій області.
3. Дії ***злочинного*** порушника найнебезпечніші. Він здатний не тільки руйнувати, але й створювати хибні СП. Історія протистояння розвідки й контррозвідки знає чимало прикладів, коли реалізація цієї погрози приводила до катастрофічних наслідків. Ця погроза актуальна й стосовно систем ЦВЗ. Володіючи здатністю створювати водяні знаки, порушник може створювати копії контенту, що захищається, створювати хибні оригінали й т.д.

Для здійснення тієї або іншої погрози порушник застосовує атаки.

Найбільш проста атака - ***суб'єктивна***. Порушник уважно розглядає зображення (слухає аудіозапис), намагаючись визначити “на око”, чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти зовсім незахищених стеганосистем, проте, вона найпоширеніша на практиці, принаймні, на початковому етапі розкриття стеганосистеми.

Для більшості сучасних методів, які використовуються для приховання повідомлень у файлах цифрового формату при організації прихованого каналу зв'язку, має місце залежність надійності сприйняття СП від обсягу даних, що вбудовуються, представлена на рис.3.2, де очевидним є той факт, що збільшення обсягу даних, що вбудовуються, значно знижує надійність сприйняття СП.

Надійність сприйняття - суб'єктивна характеристика: спотворення контейнера за рахунок вбудови ДІ не повинне бути помітно людині. Таким чином, у систему стеганографічної передачі даних включається людина, що вносить додаткові, неподоланні до цього моменту труднощі у процес математичної формалізації забезпечення розглянутої вимоги, хоча робота в цьому напрямку ведеться дуже активно, із залученням великого математичного апарата.

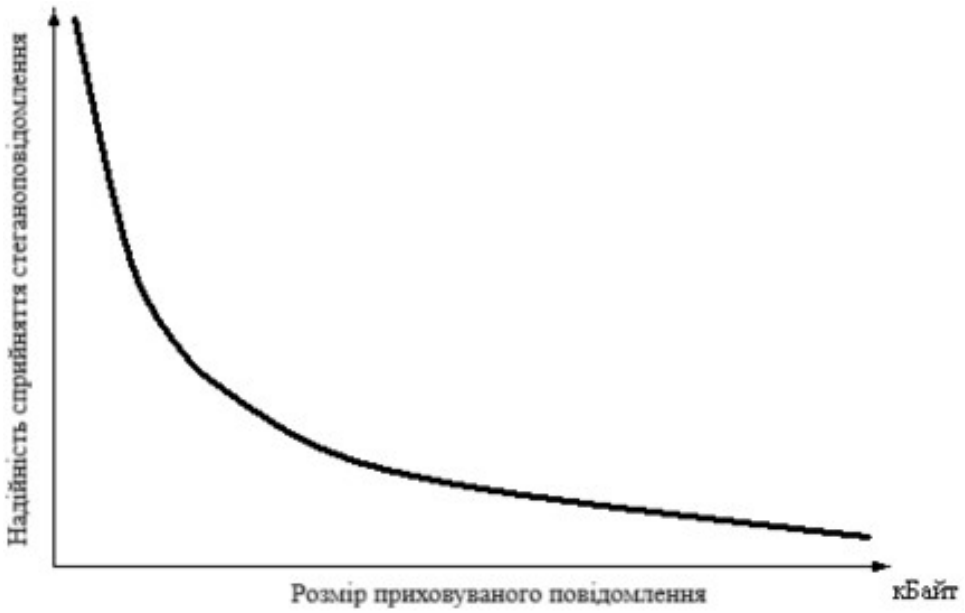


Рис. 3.2. Взаємозв'язок між надійністю сприйняття стеганоповідомлення й обсягом приховуваного повідомлення при незмінному розмірі контейнера

Нехай у якості контейнера розглядається зображення в градаціях сірого, $n \times n$-матриця якого позначається F. Вбудову ДІ в контейнер, незалежно від способу й області цієї вбудови відповідно до матеріалу Теми 2, можна представити як збурення ΔF поданої матриці F. Матриця стеганоповідомлення $\overline{F}$ очевидно задовольняє співвідношенню (2.3), де $\Delta F = f(F)$, тобто ΔF є деякою функцією F.

Будь-які перетворення, які проводяться над СП при його транспортуванні або зберіганні, включаючи активні атакуючі дії, будемо розглядати як додаткові збурення матриці контейнера F.

Дотепер при аналізі рівня візуальних спотворень, які вносяться в контейнер при стегоперетворенні, широко застосовуються **різницеві показники**, що ґрунтуються на різних модифікаціях відношення «сигнал-шум»:

- відношення «сигнал-шум»: $SNR = \dfrac{\|F\|_F^2}{\|\Delta F\|_F^2}$;
- максимальне (пікове) відношення «сигнал-шум»: $PSNR = \dfrac{n^2 \max\limits_{i,j} f_{ij}^2}{\|\Delta F\|_F^2}$;
- якість зображення: $IF = 1 - \dfrac{\|\Delta F\|_F^2}{\|F\|_F^2}$,

хоча слабкі місця таких показників давно відомі (наприклад, відсутність кореляції цих показників із зором людини). Як видне з наведеного на рис.3.3 ілюстративного прикладу, пікове відношення «сигнал-шум» PSNR може бути значним, але при цьому відбувається явне порушення надійності сприйняття (рис.3.3(б)), а при набагато меншому значенні PSNR видимі зміни на ЦЗ не спостерігаються.

Широке використання різницевих показників спотворення ЦЗ пояснюється тим, що всі існуючі моделі зорового сприйняття є лише частковим і обмеженим

відображенням зорової системи людини в силу її складності, а показники спотворення, засновані на таких моделях, інформація про які доступна з відкритих джерел, усе ще залишаються недосконалими й досить складними в реалізації.

а

б

в

Рис.3.3. Ілюстрація недосконалості різницевих показників для оцінки візуальних спотворень ЦЗ: а - вхідне ЦЗ, б - спотворене ЦЗ (*PSNR* = 48 *dB*), в – спотворене за допомогою гауссівського шуму ЦЗ (*PSNR* =28 *dB*)

Суб'єктивна атака, будучи однією з найпоширеніших стеганографічних атак, не єдина. За аналогією із криптоаналізом у стеганографії можна виділити наступні атаки:

- *Атака на основі відомого заповненого контейнера*. У цьому випадку в порушника є одне або декілька СП. В останньому випадку передбачається, що вбудова приховуваної інформації здійснювалося одним способом. Завдання порушника може полягати у виявленні факту наявності стеганоканалу (основна), а також у його декодуванні або визначенні ключа. Знаючи ключ, порушник одержить можливість аналізу інших стеганоповідомлень.
- *Атака на основі відомого вбудованого повідомлення*. Цей тип атаки більшою мірою характерний для систем захисту інтелектуальної власності, коли в якості водяного знака використовується відомий логотип фірми. Завданням

аналізу є отримання ключа. Якщо відповідний до прихованого повідомлення заповнений контейнер невідомий, то завдання розв'язується вкрай важко.

- *Атака на основі обраного прихованого повідомлення*. У цьому випадку порушник має можливість пропонувати для передачі свої повідомлення й аналізувати СП, які виходять.
- *Атака на основі обраного заповненого контейнера*. Цей тип атаки більше характерний для систем ЦВЗ. Стегоаналітик має детектор СП у вигляді «чорного ящика» і декілька СП. Аналізуючи детектовані приховані повідомлення, порушник намагається розкрити ключ.

У порушника може бути можливість застосувати ще три атаки, що не мають прямих аналогій у криптоаналізі:

- *Атака на основі відомого порожнього контейнера*. Якщо він відомий порушникові, то шляхом порівняння його з передбачуваним СП він завжди може встановити факт наявності стеганоканалу. Незважаючи на тривіальність цього випадку, у ряді робіт приводиться його інформаційно-теоретичне обґрунтування. Набагато цікавіше сценарій, коли контейнер відомий приблизно, з деякою похибкою (як це може мати місце при додаванні до нього шуму).
- *Атака на основі обраного порожнього контейнера*. У цьому випадку порушник здатний змусити користуватися запропонованим їм контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити таємність вбудови.
- *Атака на основі відомої математичної моделі контейнера або його частини*. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад, припустимо, що біти усередині зображення коррельовані. Тоді відсутність такої кореляції може служити сигналом про наявне приховане повідомлення. Завдання того, хто вбудовує повідомлення, полягає в тому, щоб не порушити статистики контейнера. Ті, хто вбудовує ДІ, і атакує, можуть мати у своєму розпорядженні різні моделі сигналів, тоді у противоборстві переможе той, хто має кращу модель.

Розглянуті вище атаки мають одну особливість: вони не змінюють стеганоповідомлення, дії порушника навряд чи здатні насторожити відправника й одержувача.

Атаки іншого типу - це *атаки проти вбудованого повідомлення*, які змінюють стеганоповідомлення, а значить можуть змінити й вбудовану в контейнер інформацію. Однією з таких атак є атака, заснована на застосуванні алгоритму стиску Jpeg до СП.

Геометричні атаки - найнебезпечніші на сьогоднішній день, вони змінюють стеганоповідомлення шляхом внесення просторових або часових спотворень, також будучи атаками проти вбудованого повідомлення. Геометричні атаки математично моделюються як аффінні перетворення з невідомим декодеру параметром. Аффінні перетворення: масштабування, зміна пропорцій, повороти, зсув й усікання. Ці атаки приводять до втрати синхронізації в детекторі ДІ й можуть бути локальними або глобальними (тобто застосованими до всього сигналу). При цьому можливо вирізання окремих

пікселів або рядків, перестановка їх місцями, застосування якихось перетворень і т.д.

Перераховані стеганографічні атаки не вичерпують усього їх різноманіття, будучи найбільше широко й часто використовуваними.

5. Пропускна спроможність каналів передачі прихованої інформації

Для стеганографічних систем важливо визначити, наскільки великою може бути пропускна спроможність каналів передачі приховуваних повідомлень, і як вона залежить від інших характеристик стеганосистем і умов їх використання. Неформально визначимо, що під *пропускною спроможністю* каналів передачі приховуваних повідомлень або просто пропускною спроможністю прихованого каналу зв'язку (ПСПК) будемо розуміти максимальну кількість інформації, яка може бути вкладене в один елемент контейнера. Канал прихованого зв'язку утворюється усередині каналу відкритого зв'язку (каналу загального користування). Пропускна спроможність каналу відкритому зв'язку визначається як кількість інформації, яку потенційно можна передати без помилок за одне використання каналу. При цьому не пред'являється ніяких вимог до захищеності від атак організованого порушника. Тому логічно припустити, що ПСПК повинна бути менше пропускної спроможності каналу відкритого зв'язку, у якому за одне використання каналу передається один елемент контейнера, у який вкладена приховувана інформація.

6. Поняття стійкості стеганосистеми

У порівнянні з достатньо добре дослідженими криптографічними системами, поняття й оцінки безпеки стеганографічних систем більш складні й допускають більше число їх тлумачень. Зокрема, це пояснюється як недостатнім теоретичним і практичним проробленням питання безпеки стеганосистем, так і великою різноманітністю завдань стеганографічного захисту інформації.

Як і для криптографічних систем захисту інформації, безпека стеганосистем описується й оцінюється їхньою стійкістю (стеганографічною стійкістю або для стислості стеганостійкістю).

Під ***стійкістю*** різних стеганосистем розуміється їхня здатність приховувати від кваліфікованого порушника факт прихованої передачі повідомлень, здатність протистояти спробам порушника зруйнувати, спотворити, вилучити потай передані повідомлення, а також здатність підтвердити або спростувати автентичність потай переданої інформації.

Дослідимо стегосистеми, завданням яких є прихована передача інформації. У криптографічних системах ховається зміст конфіденційного повідомлення від порушника, у той час як у стеганографії додатково ховається факт існування такого повідомлення. Тому визначення стійкості й злому цих систем різні. У криптографії система захисту інформації є стійкою, якщо, маючи перехоплену криптограму, порушник не здатний читати повідомлення, що міститься в ній. Неформально визначимо, що ***стеганосистема є стійкою, якщо порушник, спостерігаючи інформаційний обмін між відправником і одержувачем, не здатний виявити, що під прикриттям контейнерів передаються приховувані повідомлення, і тим більше читати ці повідомлення***.

Назвемо в загальному випадку стеганосистему нестійкою, якщо протиборча сторона здатна виявляти факт її використання.

Безпека стеганосистем (за принципом Керхгоффа) повинна опиратися на такі принципи їх побудови, при яких, якщо порушник не знає секретної ключової інформації, то навіть при повному знанні функцій вбудовування й витягу приховуваної інформації, законів розподілу приховуваних повідомлень, контейнерів і СП, він не здатний установити факт прихованої передачі інформації.

Стійкість різних стеганосистем може бути розділена на:

- стійкість до виявлення факту передачі (існування) приховуваної інформації,
- стійкість до витягу приховуваної інформації,
- стійкість до нав'язування хибних повідомлень по каналу прихованого зв'язку (імітостійкість),
- стійкість до відновлення секретного ключа стегосистеми,
- стійкість до атак проти вбудованого повідомлення.

Очевидно, що якщо стеганосистема є стійкою до виявлення факту передачі (існування) приховуваної інформації, то логічно припустити, що вона при цьому є стійкою й до читання приховуваної інформації. Зворотне в загальному випадку невірно. Стеганосистема може бути стійкою до читання приховуваної інформації, але факт передачі інформації під прикриттям контейнера може виявлятися порушником.

Стійкість стеганосистеми до нав'язування хибних повідомлень по каналу прихованого зв'язку характеризує її здатність виявляти й відкидати сформовані порушником повідомлення, що вводяться їм у канал передачі приховуваних повідомлень із метою видачі їх за оригінальні, такі, що виходять від законного відправника. Якщо в системі ДІ зловмисник здатний увести в контейнер, завірений законним відправником, свій водяний знак, і детектор буде виявляти водяний знак зловмисника й не виявляти ЦВЗ дійсного відправника, то це означає дискредитацію (злом) системи ЦВЗ.

Стійкість до відновлення секретного ключа стеганосистеми характеризує її здатність протистояти спробам порушника обчислити секретну ключову інформацію даної стеганосистеми. Якщо порушник здатний визначити ключ стеганосистеми, то він може однозначно виявляти факти передачі приховуваних повідомлень і читати їх або нав'язувати хибні повідомлення без усяких обмежень. Таку подію можна назвати повною компрометацією стеганосистеми. Очевидно, що атаки порушника на ключ стеганосистеми можуть бути побудовані аналогічно атакам на ключ систем шифрування інформації й систем автентифікації повідомлень.

Стійкість стеганосистеми до атак проти вбудованого повідомлення вже обговорювалася вище.

7. Локалізація області збурень параметрів стеганоповідомлення для забезпечення певних властивостей стеганосистеми

7.1. Забезпечення надійності сприйняття стеганоповідомлення

Стеганоперетворення як збурення набору параметрів, що визначають основне повідомлення. Розглянемо докладно процес стеганоперетворення дискретного двовимірного сигналу (ЦЗ або кадра цифрового відео). У якості контейнера, не обмежуючи спільності міркувань, для простоти викладу розглядається зображення, формальним представленням якого є одна матриця F. Перетворення контейнера за рахунок вбудови в нього ДІ, незалежно від способу й області цієї вбудови, можна представити у вигляді (2.3), тобто довільне СПр можна представити у вигляді аддитивної вбудови деякої інформації в просторовій області.

Будь-які перетворення, які проводяться над СП, будемо розглядати як додаткові збурення матриці ОП F. Відповідно до наведеного вище:

- СПр вхідного контейнера, а також будь-які перетворення СП при його пересиланні або зберіганні, включаючи активні атакуючі дії, представляються у вигляді елементарних матричних операцій.
- Довільне СПр представляється у вигляді збурення СНЧ і (або) СНВ матриці ОП, що визначаються нормальним сингулярним розкладанням матриці (рис.2.1 (Тема 2));
- СПр представляється у вигляді збурення спектра й (або) ВВ матриці ОП, що визначаються нормальним спектральним розкладанням, у випадку симетричної матриці контейнера.

Основною задачею будь-якого стеганоалгоритма є забезпечення збереження в секреті наявності таємного каналу передачі інформації, інакше кажучи, згенероване стеганографічним алгоритмом СП повинно зберігати надійність сприйняття: спотворення контейнера за рахунок вбудови ДІ не повинно бути помітним.

Вплив норми матриці збурення на процес забезпечення надійності сприйняття стеганоповідомлення. Базисним перетворенням, що використовуються в багатьох сучасних алгоритмах стиску графічної інформації, а також стеганографічних алгоритмах, є дискретне косинусне перетворення (ДКП), яке можемо записати в матричній формі

$$S = C_N X C_N^T, \tag{3.1}$$

де X — фрагмент поданого ЦЗ розміру $N \times N$,

C — $N \times N$-матриця ДКП, елементи $C(i,j),\ i,j = 0,1,...,N-1$ якої обчислюються за формулою:

$$C(i,j) = \begin{cases} \dfrac{1}{\sqrt{N}}, & \text{при } i = 0; \\ \sqrt{\dfrac{2}{N}} \cos(2j+1) \cdot i \cdot \pi, & \text{при } i > 0. \end{cases}$$

У результуючій матриці S (3.1) ДКП має місце наступний розподіл частотних складових, схематично показаний на рис. 3.4.

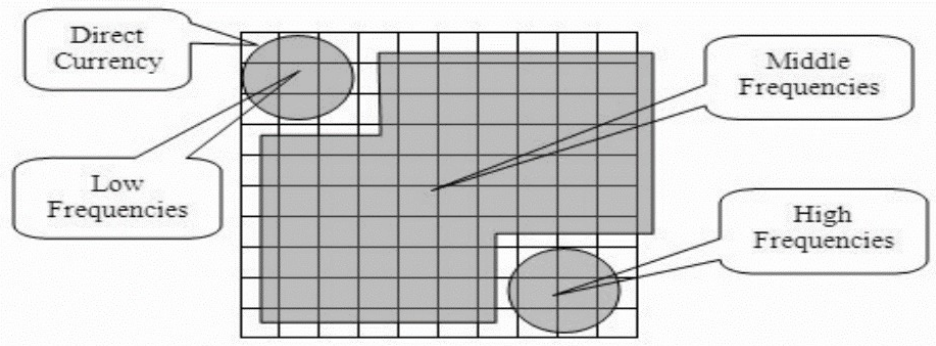


Рис. 3.4. Розподіл частотних складових у трансформантах ДКП

Загальновідомо, що модифікація високочастотних складових (розташованих у нижньому правому куті матриці трансформант ДКП) веде до найменших візуальних спотворень вхідного зображення, тоді як модифікація середніх частот відповідає більшим спотворенням. Найбільші спотворення вхідного зображення відбуваються при модифікації низькочастотних складових (лівий верхній кут) матриці трансформант ДКП.

В існуючих стеганометодах часто зустрічаються обмеження на область їх застосовності саме через те, що для якихось ЦЗ-контейнерів надійність сприйняття формованого СП може порушуватися. Це найчастіше відбувається в силу того, що при розробці стеганоалгоритма не враховуються достатні формальні умови такого забезпечення (або такі формальні умови у використовуваній області контейнера не знайдені), а оцінка надійності сприйняття робиться вже апостеріорно, по факту. Така ситуація не дає повною мірою можливості використання випадкового контейнера, є недоліком цих методів.

Оскільки СПр ОП, а також збурні дії, яким зазнає СП, повинні забезпечувати надійність його сприйняття, то $\|\Delta F\|$ не може бути нескінченно великою, де ΔF — матриця збурення контейнера або СП, оскільки у цьому випадку достовірною подією виявиться порушення висунутої вимоги. Крім того, при $\|\Delta F\| \to 0$ імовірність забезпечення надійності сприйняття буде прямувати до одиниці для кожного ОП. Значення різницевих показників для зображення з матрицею F визначаються величиною $\|\Delta F\|_F$: чим менше $\|\Delta F\|_F$, тим краще кількісний показник візуального спотворення F, що отримується при використанні кожного з них. Враховуючи це, висувається наступна гіпотеза, яка підтверджується обчислювальним експериментом: чим менше $\|\Delta F\|_F$, тим більше ймовірність забезпечення надійності сприйняття для зображення з матрицею $F + \Delta F$ при заданому зображенні F, до того ж замість $\|\Delta F\|_F$ можна використовувати $\|\Delta F\|_2$ - спектральна матрична норма.

Умови забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера. Розглядаючи матрицю контейнера як симетричну (Тема 2), позначимо її A, щоб відрізняти від довільної матриці F.

Теорема 1. Нехай вбудова ДІ викликає збурення $\delta_{k_1},...,\delta_{k_p}$ ВЗ $\lambda_{k_1},...,\lambda_{k_p}$ матриці A контейнера. Тоді величина норми матриці збурення ΔA не залежить від того, які саме ВЗ були збурені, а залежить лише від абсолютних величин цих збурень.

Доказ. Позначимо $\overline{A}$ матрицю СП, що отримане на основі A. Якщо $A = U\Lambda U^T$ - спектральне розкладання матриці контейнера, яке може бути представленим у формі зовнішніх добутків $A = \sum_{i=1}^{n} \lambda_i u_i u_i^T$, то спектральне розкладання матриці СП $\overline{A}$ буде мати вигляд:

$$\overline{A} = U\, diag(\lambda_1,...,\lambda_{k_1-1},\lambda_{k_1}+\delta_{k_1},\lambda_{k_1+1},...,\lambda_{k_p-1},\lambda_{k_p}+\delta_{k_p},\lambda_{k_p+1},...,\lambda_n)U^T.$$

Тоді

$$\Delta A = \overline{A} - A = \sum_{j=1}^{p} \delta_{k_j} u_{k_j} u_{k_j}^T, \quad \|\Delta A\|_2 = \max_{1\le j\le p} |\delta_{k_j}|.$$

Зв'язок між $\|\Delta A\|$ і $\delta_{k_1},...,\delta_{k_p}$ залежить від вибору матричної норми. Наприклад, якщо розглянути норму Фробеніуса, то

$$\|\Delta A\|_F = \left\| \sum_{j=1}^{p} \delta_{k_j} u_{k_j} u_{k_j}^T \right\|_F \le \sum_{j=1}^{p} |\delta_{k_j}| \|u_{k_j}\|_2 \|u_{k_j}^T\|_2 = \sum_{j=1}^{p} |\delta_{k_j}| \le p \max_{1\le j\le p} |\delta_{k_j}|,$$

висновок теореми істинний.

Теорема 2. Нехай СПр викликало збурення ВВ матриці A контейнера. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ малим по модулю ВЗ A.

Без доказу.

Нехай ΔA — збурення матриці A тільки за рахунок збурення ВВ, $u_i, \overline{u_i}$ — нормовані даний і збурений ВВ, що відповідають λ_i, а θ_i — кут між ними.

Теорема 3. Нехай СПр збурило ВВ матриці A ОП. Достатньою умовою для забезпечення малого значення норми матриці збурення є відповідність збурених ВВ власним значенням матриці ОП із малою абсолютною відокремленістю.

Доказ. Оскільки нерівність (1.10) має місце для кожного ВЗ матриці A, то

$$\max_{1\le i\le n} \left(\frac{1}{2} \sin\theta_i \, gap_{abs}(i, A) \right) \le \|\Delta A\|_2, \qquad (3.2)$$

звідки випливає висновок теореми. З формули (3.2) випливає, що якщо при збуренні вхідної матриці A її ВЗ не міняються або міняються незначно, то

навіть великі збурення ВВ, що відповідають погано абсолютно відокремленим СЗ ($gap_{abs}(i,A)$ мала), приведуть до малого значення $\|\Delta A\|_2$.

З метою забезпечення великої ймовірності надійності сприйняття СП вбудову ДІ в контейнер доцільно робити таким чином, щоб збурені стеганоперетворенням ВВ відповідали малим по модулю ВЗ або ВЗ, що мають малі абсолютні відокремленості, збурення ВЗ були малі. Чим менше збурення ВЗ, абсолютні відокремленості й модулі ВЗ, що відповідають збуреним ВВ, тим більше ймовірність дотримання надійності сприйняття СП.

Аналогічна умова може бути отримана для контейнера з довільною матрицею з використанням її СНЧ і СНВ (див. «Методичні вказівки до лабораторних робіт»).

Відповідність між параметрами двовимірного сигналу в різних областях перетворення

Визначення. Назвемо

$$F_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$$

апроксимацією ранга k зображення F,

$$F_{k_d} = \sum_{i=k+1}^{n} \sigma_i u_i v_i^T$$

доповненням до апроксимації F_k,

$$S_k = \sigma_k u_k v_k^T$$

k ***-ою складовою*** зображення F.

На прикладі зображення CAMERAMAN розглянемо апроксимації різного рангу, а також доповнення до апроксимацій (рис.3.5). Результати візуально аналогічні результатам низькочастотної (рис.3.5(б,в)) і високочастотної фільтрації (рис.3.5). Варіанти *а* і *г* (рис.3.5) наочно не відрізняються один від іншого.

Виходячи з розглянутих результатів, висувається гіпотеза: сингулярні трійки, що відповідають найбільшим СНЧ, відповідають головним чином низькочастотним, а найменшим - високочастотним складовим сигналу.

Для перевірки гіпотези був проведений обчислювальний експеримент, у якому використовувалися 10000 різних по розміру, яскравості, фактурі і т.д. зображень у градаціях сірого. Для наочності ілюстрації основних результатів розглянемо як вхідне зображення головну підматрицю WW матриці F розміру 11×11 певного ЦЗ, що дає типову якісну картину. Будемо позначати матрицю центрованого енергетичного спектра довільної матриці A як $SPECTR(A)$. Розглянемо для WW центровані енергетичні спектри деяких її складових, апроксимацій і доповнень до апроксимацій (рис.3.6 — виділені найбільші й найменші значення спектральних коефіцієнтів). Як видне з наведених результатів, сингулярні трійки, що відповідають максимальним СНЧ, відповідають, головним чином, низькочастотним складовим сигналу-зображення. Разом із зменшенням СНЧ відбувається підключення середніх і високих частот, а внесок низьких стає усе менше. Найменші СНЧ відповідають високочастотним складовим двовимірного цифрового сигналу.

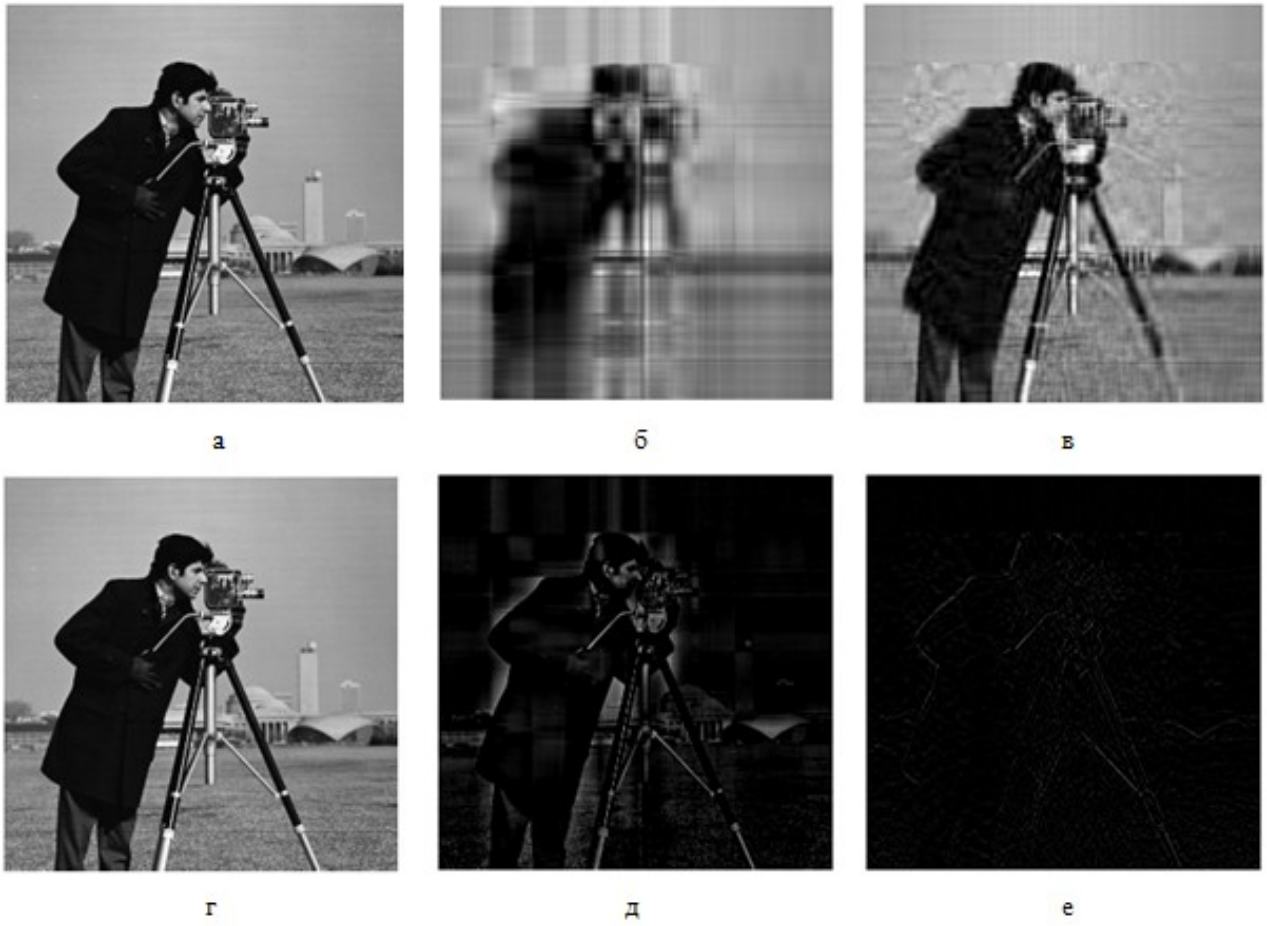


Рис.3.5. Зображення CAMERAMAN і його апроксимації: первісне зображення (а); F_5 (б); F_{20} (в); F_{150} (г); F_{5_d} (д); F_{40_d} (е)

Перевіримо, як реагує енергетичний спектр вхідного зображення WW на збурення різних СНЧ. При проведенні обчислювального експерименту збурення найбільших СНЧ приводили до збурень у центральній частині матриці центрованого спектра, залишаючи практично незмінними високочастотні складові. При збуренні малих СНЧ, картина змінювалася на протилежну: значно збурювалися високочастотні складові енергетичного спектра й практично не зачіпалися інші частотні складові. Наприклад, якщо значення $\sigma_{10} = 0.5704$ покласти рівним 0.0008, матриця відносних збурень (погрішностей) кожного елемента центрованого енергетичного спектра, обчислених у відсотках, буде мати вигляд (жирним шрифтом виділені максимальні відносні погрішності):

23.6480	**4.4449**	**4.4375**	0.7313	0.9534	0.0026	0.1649	0.6653	0.0679	**15.8227**	**2.4734**
61.7384	**5.6856**	1.0781	1.2315	1.2946	0.0004	0.1883	1.3749	0.3244	**2.6020**	**5.8417**
2.8855	1.8952	1.1789	3.0755	0.1963	0.0002	0.1284	0.9665	0.2908	1.7989	**4.9052**
0.3363	0.1977	0.0943	0.0294	0.0042	0.0000	0.0073	0.0425	0.0405	0.1022	0.2421
1.8512	0.3385	0.0985	0.0669	0.0065	0.0000	0.0124	0.0950	0.1105	1.6317	2.2347
0.0000	0.0037	0.0018	0.0011	0.0002	0.0000	0.0002	0.0011	0.0018	0.0037	0.0000
2.2347	1.6317	0.1105	0.0950	0.0124	0.0000	0.0065	0.0669	0.0985	0.3385	1.8512
0.2421	0.1022	0.0405	0.0425	0.0073	0.0000	0.0042	0.0294	0.0943	0.1977	0.3363
4.9052	1.7989	0.2908	0.9665	0.1284	0.0002	0.1963	3.0755	1.1789	1.8952	**2.8855**
5.8417	**2.6020**	0.3244	1.3749	0.1883	0.0004	1.2946	1.2315	1.0781	**5.6856**	**61.7384**
2.4734	**15.8227**	0.0679	0.6653	0.1649	0.0026	0.9534	0.7313	**4.4375**	**4.4449**	**23.6480**

$SPECTR(S_1) =$

1.0e+004 *

0.0000	0.0000	0.0000	0.0000	0.0000	0.0015	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0024	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0001	0.0001	0.0072	0.0001	0.0001	0.0000	0.0000	0.0000
0.0001	0.0001	0.0001	0.0001	0.0003	**0.0136**	0.0003	0.0001	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0002	**0.0161**	**0.0217**	**0.0161**	0.0002	0.0001	0.0001	0.0001
0.0060	0.0067	0.0082	0.0145	**0.0265**	**1.3294**	**0.0265**	0.0145	0.0082	0.0067	0.0060
0.0001	0.0001	0.0001	0.0002	**0.0161**	**0.0217**	**0.0161**	0.0002	0.0001	0.0001	0.0001
0.0001	0.0001	0.0001	0.0001	0.0003	**0.0136**	0.0003	0.0001	0.0001	0.0001	0.0001
0.0000	0.0000	0.0000	0.0001	0.0001	0.0072	0.0001	0.0001	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0024	0.0000	0.0000	0.0000	0.0000	0.0000
0.0000	0.0000	0.0000	0.0000	0.0000	0.0015	0.0000	0.0000	0.0000	0.0000	0.0000

$SPECTR(S_4) =$

3.5943	10.1517	9.9107	10.4392	7.9704	0.2183	7.9704	10.4392	9.9107	10.1517	3.5943
2.1460	6.0612	5.9173	6.2328	4.7588	0.1304	4.7588	6.2328	5.9173	6.0612	2.1460
5.5889	15.7850	15.4103	16.2320	12.3933	0.3395	12.3933	16.2320	15.4103	15.7850	5.5889
8.8097	24.8817	24.2910	25.5863	19.5354	0.5351	19.5354	25.5863	24.2910	24.8817	8.8097
12.4076	35.0435	34.2116	36.0358	27.5137	0.7537	27.5137	36.0358	34.2116	35.0435	12.4076
0.0077	0.0218	0.0213	0.0224	0.0171	0.0005	0.0171	0.0224	0.0213	0.0218	0.0077
12.4076	35.0435	34.2116	36.0358	27.5137	0.7537	27.5137	36.0358	34.2116	35.0435	12.4076
8.8097	24.8817	24.2910	25.5863	19.5354	0.5351	19.5354	25.5863	24.2910	24.8817	8.8097
5.5889	15.7850	15.4103	16.2320	12.3933	0.3395	12.3933	16.2320	15.4103	15.7850	5.5889
2.1460	6.0612	5.9173	6.2328	4.7588	0.1304	4.7588	6.2328	5.9173	6.0612	2.1460
3.5943	10.1517	9.9107	10.4392	7.9704	0.2183	7.9704	10.4392	9.9107	10.1517	3.5943

$SPECTR(S_{10}) =$

1.8525	**1.1453**	0.5306	0.6668	0.1127	0.0007	0.1127	0.6668	0.5306	**1.1453**	**1.8525**
1.0079	0.6231	0.2887	0.3628	0.0613	0.0004	0.0613	0.3628	0.2887	0.6231	**1.0079**
1.2189	0.7536	0.3492	0.4387	0.0742	0.0005	0.0742	0.4387	0.3492	0.7536	**1.2189**
0.1168	0.0722	0.0335	0.0421	0.0071	0.0000	0.0071	0.0421	0.0335	0.0722	0.1168
0.4630	0.2863	0.1326	0.1667	0.0282	0.0002	0.0282	0.1667	0.1326	0.2863	0.4630
0.0119	0.0073	0.0034	0.0043	0.0007	0.0000	0.0007	0.0043	0.0034	0.0073	0.0119
0.4630	0.2863	0.1326	0.1667	0.0282	0.0002	0.0282	0.1667	0.1326	0.2863	0.4630
0.1168	0.0722	0.0335	0.0421	0.0071	0.0000	0.0071	0.0421	0.0335	0.0722	0.1168
1.2189	0.7536	0.3492	0.4387	0.0742	0.0005	0.0742	0.4387	0.3492	0.7536	**1.2189**
1.0079	0.6231	0.2887	0.3628	0.0613	0.0004	0.0613	0.3628	0.2887	0.6231	**1.0079**
1.8525	**1.1453**	0.5306	0.6668	0.1127	0.0007	0.1127	0.6668	0.5306	**1.1453**	**1.8525**

$SPECTR(WW_2) =$

1.0e+004 *

0.0000	**0.0002**	**0.0003**	**0.0007**	**0.0008**	0.0015	**0.0008**	**0.0006**	**0.0003**	**0.0002**	**0.0000**
0.0001	**0.0002**	**0.0004**	**0.0008**	0.0011	0.0024	0.0011	**0.0008**	**0.0004**	**0.0002**	**0.0000**
0.0001	**0.0005**	**0.0009**	0.0018	0.0023	0.0071	0.0023	0.0018	**0.0009**	**0.0004**	**0.0001**
0.0004	0.0015	0.0031	0.0062	0.0079	**0.0132**	0.0079	0.0062	0.0030	0.0015	**0.0003**
0.0008	0.0034	0.0070	**0.0142**	**0.0179**	**0.0206**	**0.0179**	**0.0142**	0.0070	0.0035	**0.0008**
0.0060	0.0067	0.0079	**0.0139**	**0.0257**	**1.3294**	**0.0257**	**0.0139**	0.0079	0.0067	0.0060
0.0008	0.0035	0.0070	**0.0142**	**0.0179**	**0.0206**	**0.0179**	**0.0142**	0.0070	0.0034	**0.0008**
0.0003	0.0015	0.0030	0.0062	0.0079	**0.0132**	0.0079	0.0062	0.0031	0.0015	**0.0004**
0.0001	**0.0004**	**0.0009**	0.0018	0.0023	0.0071	0.0023	0.0018	**0.0009**	**0.0005**	**0.0001**
0.0000	**0.0002**	**0.0004**	**0.0008**	0.0011	0.0024	0.0011	**0.0008**	**0.0004**	**0.0002**	**0.0001**
0.0000	**0.0002**	**0.0003**	**0.0006**	**0.0008**	0.0015	**0.0008**	**0.0007**	**0.0003**	**0.0002**	**0.0000**

$SPECTR(WW_{9d}) =$

1.8306	**1.3008**	**0.8762**	**0.7004**	0.2120	**0.0010**	0.1365	0.6360	**0.8354**	**0.9764**	**1.7938**
1.1550	**1.5701**	**0.7467**	0.5350	0.4071	**0.0006**	0.3099	0.2409	**0.6105**	**0.7124**	**0.9900**
1.3455	**1.8184**	**1.0021**	0.6491	0.4571	**0.0009**	0.3106	0.2299	0.8401	0.3811	**1.1132**
0.1548	0.5956	0.4820	**0.1032**	**0.2211**	**0.0005**	**0.2301**	**0.1549**	0.4931	0.6850	0.2113
0.4583	0.2072	**0.0930**	**0.1442**	**0.0358**	**0.0001**	**0.0786**	**0.1919**	**0.1471**	0.4248	0.4847
0.0118	**0.0072**	**0.0041**	**0.0043**	**0.0007**	**0.0000**	**0.0007**	**0.0043**	**0.0041**	**0.0072**	0.0118
0.4847	0.4248	**0.1471**	**0.1919**	**0.0786**	**0.0001**	**0.0358**	**0.1442**	**0.0930**	0.2072	0.4583
0.2113	0.6850	0.4931	**0.1549**	**0.2301**	**0.0005**	**0.2211**	**0.1032**	0.4820	0.5956	0.1548
1.1132	0.3811	0.8401	0.2299	0.3106	**0.0009**	0.4571	0.6491	**1.0021**	**1.8184**	**1.3455**
0.9900	**0.7124**	**0.6105**	0.2409	0.3099	**0.0006**	0.4071	0.5350	**0.7467**	**1.5701**	**1.1550**
1.7938	**0.9764**	**0.8354**	0.6360	0.1365	**0.0010**	0.2120	**0.7004**	**0.8762**	**1.3008**	**1.8306**

Рис.3.6. Матриці центрованих енергетичних спектрів

Таким чином, результати експерименту повністю підтвердили висунуту гіпотезу.

Враховуючи, що будь-яке СПр ОП еквівалентним чином представляється у вигляді збурень СНЧ і (або) СНВ матриці ОП, однозначно визначаємих нормальним SVD, зв'язок між енергетичним спектром сигналу й сингулярними трійками його матриці й той факт, що при вбудові ДІ в частотній області ОП

для забезпечення стійкості стеганометоду до збурень і надійності сприйняття СП пріоритетної є модифікація середньої частини частотного спектра, можна зробити висновок, що аналогічними з погляду стійкості виявляться стеганометоди, для яких СПр збурить сингулярні трійки, що відповідають середнім за значенням сингулярним числам матриці ОП (відповідних до середньої частини частотного спектра контейнера), незалежно від безпосередньо використовуваної цими методами області вбудови ДІ.

7.2. Чутливість стеганоповідомлення до збурних дій

Умова нечутливості стеганоповідомлення до збурних дій. Одна з основних вимог, що висуваються до будь-якого СП із метою забезпечення ефективного декодування секретної інформації, - нечутливість до збурних дій.

Визначення. СП будемо називати *чутливим*, якщо навіть незначні збурні дії, яких воно зазнає, здатні зруйнувати значну частину вбудованої ДІ й привести до виникнення великої кількості помилок при декодуванні ДІ, і *нечутливим* інакше.

Скрізь нижче розглядаються такі збурення, що впливають на контейнер і СП, які забезпечують високу ймовірність забезпечення надійності сприйняття, - *малі збурні дії*.

Серед стеганоалгоритмів приховання даних у ЦЗ найбільш популярними є узагальнені групи методів, що працюють у просторовій і частотній областях. Більш стійкими до різноманітних спотворень вважаються методи другої групи, що апріорі забезпечує «програшну» з погляду стійкості позицію стеганоалгоритмам із першої групи, хоча використання області первинного зображення, що не вимагає яких-небудь додаткових витрат для побудови різних його перетворень, в обчислювальному сенсі є більш привабливим.

Однак, з огляду на матеріал Теми 2, а саме на основи ЗПАІС, можна стверджувати, що стійкість стеганоалгоритмів до збурних дій, як і інші властивості, визначається не використовуваною областю вбудови ДІ, а локалізацією збурень СНЧ (ВЗ) і СНВ (ВВ), що відбулися в результаті СПр контейнера.

Нехай F — матриця контейнера.

Визначення. Стеганоалгоритм назвемо *нестійким*, якщо малі збурні дії можуть привести до значного або повного знищенню вбудованої в контейнер за допомогою цього алгоритму секретної інформації, і *стійким* інакше.

Таким чином, стеганоалгоритм буде нестійким, якщо згенероване їм СП буде чутливим до збурень.

Нехай СПр, що здійснюється деяким стеганоалгоритмом, збурило СНВ матриці контейнера. ***Достатньою умовою забезпечення малої чутливості одержуваного СП до збурень, а тому стійкості використовуваного стеганоалгоритму, незалежно від області вбудови ДІ (просторової або області якого-небудь перетворення), є відповідність збурених СНВ сингулярним числам з великою відокремленістю. Відокремленість СНЧ, що відповідають збуреним СНВ матриці ОП, є мірою чутливості отриманого СП до збурних дій***.

Наслідком з цього є наступне. Нехай $\overline{F}$ — матриця СП, результатом СПр є збурення матриці СНВ U, що отримана нормальним сингулярним розкладанням матриці F. Якщо збурення U відповідає СНВ, що відповідають СНЧ із малою відокремленістю, то одержуване СП виявиться чутливим до збурних дій, незалежно від самого алгоритму й використовуваної області вбудови ДІ.

Нехай тепер A — довільна симетрична матриця, що розглядається як матриця контейнера. Матриці СП $\overline{A}$ і довільної збурної дії E будуть розглядатися як симетричні (див. Тему 2). Для оцінки чутливості СП тут має сенс аналізувати збурення тільки ВВ при СПр матриці ОП, а ДІ представляти у вигляді сукупності цих збурень.

Достатньою умовою забезпечення малої чутливості СП до збурних дій при симетричності його матриці є відповідність збурених при СПр власних векторів контейнера власним значенням матриці СП, що мають великі абсолютні відокремленості.

Доказ. При СПр деякі (всі) ВВ матриці A контейнера збуряться, відхилившись від первісного положення на деякі кути. Це відбудеться завжди, якщо тільки алгоритм вбудови ДІ не базується на безпосередній модифікації лише ВЗ матриці контейнера. Сукупність збурень ВВ є формальним представленням для ДІ. Таким чином, чутливість отриманого СП буде визначатися чутливістю збурених при СПр ВВ матриці A. Очевидно, щоб зберегти незмінною вбудовану ДІ при збурній дії на СП, відхилення ВВ, що виникли в результаті СПр, повинні залишитися незмінними.

Нормальне спектральне розкладання (СР) матриці СП $\overline{A}$ представляється в вигляді: $\overline{A} = \overline{U}\overline{\Lambda}\overline{U}^T$. Нехай E — матриця збурення $\overline{A}$. Тоді нормальне СР симетричної матриці $\overline{A} + E$ визначається як $\overline{A} + E = \overline{\overline{U}\overline{\Lambda}\overline{U}}^T$. Нехай $\overline{u}_i, \overline{\overline{u}}_i$ — нормовані ВВ $\overline{A}$ і $\overline{A} + E$ відповідно, що відповідають $i-му$ ВЗ, а θ_i — кут між ними. Збурені при СПр контейнера ВВ, а значить і стеганоповідомлення у цілому, будуть нечутливими до збурних дій, якщо відповідні ВЗ матриці $\overline{A}$ мають великі абсолютні відокремленості, причому, чим більше $gap_{abs}(i, \overline{A})$, тим менш чутливим до збурень буде відповідний ВВ. Таким чином, абсолютні відокремленості ВЗ, що відповідають збуреним при стеганоперетвореннi ВВ, визначають чутливість отриманого СП. СП буде найменш чутливим до збурних дій, якщо СПр збурить ВВ матриці контейнера, що відповідають ВЗ матриці СП, що мають найбільші абсолютні відокремленості. Більше того, як показує обчислювальний експеримент, найбільші абсолютні відокремленості ВЗ, присутніх у спектрі матриці СП, такі, що вони забезпечують нечутливість СП у зазначеному випадку (кути повороту відповідних ВВ становлять, часто, частки градусу).

Наслідок 1. Якщо збурені в результаті стеганоперетвоення контейнера ВВ відповідають ВЗ матриці СП із малими абсолютними відокремленостями, то отримане СП виявляється чутливим до збурних дій, що, як правило, приводить до недостатньої ефективності декодування ДІ.

Враховуючи що всі збурення, що впливають на контейнер і СП, є малими, абсолютні відокремленості ВЗ матриць $\overline{A}$ і A незначно відрізняються друг від друга. Звідки випливає

Наслідок 2. Достатньою умовою забезпечення малої чутливості СП до збурень є відповідність збурених при стеганоперетворенні контейнера ВВ власним значенням матриці контейнера, що мають великі абсолютні відокремленості.

З усього вище наведено випливаєістинність наступного твердження.

Твердження. Чутливість СП до збурних дій у випадку симетричної матриці визначається чутливістю збурених ВВ матриці контейнера при СПр. Виходячи зі значень збурень ВВ і абсолютних відокремленостей відповідних ВЗ можливо зробити якісні апріорні оцінки чутливості СП до збурних дій.

Якщо матриця ЦЗ-контейнера має довільну структуру, то в якості повного набору формальних параметрів може розглядатися набір СНЧ і СНВ матриці. Тоді можна стверджувати, що

Чутливість СП до збурних дій визначається чутливістю збурених СНВ матриці контейнера при СПр. Виходячи зі значень збурень СНВ і відокремленостей відповідних СНЧ можливо зробити якісні апріорні оцінки чутливості СП до збурних дій.

Розглянемо один з стеганоалгоритмів, що задовольняє достатній умові нечутливості отримуваного стеганоповідомлення у випадку довільної матриці контейнера.

Вбудова ДІ

Крок 1. Матриця F розміром $n \times n$ ОП розбивається стандартним чином на $8 \times 8-$ блоки; B — довільний блок.

Крок 2. Нехай B - черговий блок контейнеру, що задіяний в процесі вбудови ДІ; p_i - черговий біт ДІ, що вбудовується в блок *B*:

2.1. Для B будується нормальне сингулярне розкладання: $B = U\Sigma V^T$; u_1 і v_1 — лівий і правий СНВ блока B відповідно, що відповідають максимальному СНЧ σ_1.

2.2. (*вбудова* p_i):

Якщо $p_i = 1$,

то

2.2.1. $\overline{u}_1 = n^O$, де $\overline{u}_1$ — збурений в результаті СПр u_1;

2.2.2. Обчислення $\overline{u}_2$,..., $\overline{u}_8$ — збурених $u_2,\ldots,u_8$ в процесі приведення лівих сингулярних векторів до ортонормованого з $\overline{u}_1$ виду шляхом розв'язку системи лінійних алгебраїчних рівнянь щодо елементів $\overline{u}_2$,..., $\overline{u}_8$;

інакше

2.2.1. $\overline{v}_1 = n^O$, де $\overline{v}_1$ — збурений в результаті СПр v_1;

2.2.2. Обчислення $\overline{v}_2$,..., $\overline{v}_8$ — збурених $v_2,\ldots,v_8$ в процесі приведення правих сингулярних векторів до ортонормованого з $\overline{v}_1$ виду шляхом розв'язку системи лінійних алгебраїчних рівнянь щодо елементів $\overline{v}_2$,..., $\overline{v}_8$.

2.3. (*формування блоку* $\overline{B}$ *СП, що відповідає блоку* B *контейнера*).

Якщо $p_i = 1$,

то $\overline{B} = \overline{U}\Sigma V^T$, де $\overline{U} = (n^O, \overline{u}_2, ..., \overline{u}_8)$

інакше $\overline{B} = U\Sigma\overline{V}^T$, де $\overline{V} = (n^O, \overline{v}_2, ..., \overline{v}_8)$.

Декодування ДІ.

Крок 1. Матриця СП $\overline{F}$ розміром $n \times n$ розбивається стандартним чином на $8 \times 8-$блоки; $\overline{B}$ — довільний блок.

Крок 2. З чергового блоку $\overline{B}$, що був задіяний при СПр, декодується черговий біт $\overline{p}_i$ ДІ:

2.1. Для $\overline{B}$ будується нормальне сингулярне розкладання: $\overline{B} = \overline{U}\overline{\Sigma}\overline{V}^T$; $\overline{u}_1$ і $\overline{v}_1$ — лівий і правий СНВ блока $\overline{B}$, що відповідають максимальному СНЧ $\overline{\sigma}_1$.

2.2. (*декодування* $\overline{p}_i$). Знайти UN_B і VN_B — кути між векторами $\overline{u}_1$, n^O і $\overline{v}_1$, n^O відповідно.

Якщо $UN_B < VN_B$,

то $\overline{p}_i = 1$,

інакше $\overline{p}_i = 0$.

Організація дій кроку 2.2.2 при вбудові ДІ може відбуватися наступним чином (розглянемо на прикладі матриці U (рис.3.7), де u_i^O — вектор-стовпець, ортогональний векторам $\overline{u}_1$ і $u_j^O, j = 2,..,i-1$). Забезпечення ортогональності лівих СНВ досягається шляхом розв'язку системи з 28 лінійних рівнянь з невідомими $x_i, i = \overline{1,28}$ — елементами векторів u_i^O (рис.3.7):

$$\begin{cases} \left(\overline{u}_1, u_j^O\right) = 0,\ j = 2,..,8, \\ \left(u_i^O, u_j^O\right) = 0,\ i = 2,..,8,\ j = 2,..,i-1, \end{cases}$$

де $(\bullet,\bullet)$ — скалярний добуток векторів-аргуметів. Матриця $\overline{U}$, що фігурує при формуванні матриці $\overline{B}$ блоку СП на кроці 2.3 при вбудові ДІ, включає в себе нормалізовані вектори-стовпці $\frac{u_j^O}{\left\|u_j^O\right\|}, j = 2,..,8$: $\overline{U} = \left(\overline{u}_1 \quad \frac{u_2^O}{\left\|u_2^O\right\|} \quad \frac{u_3^O}{\left\|u_3^O\right\|} \quad \cdots \quad \frac{u_8^O}{\left\|u_8^O\right\|}\right) = (n^O, \overline{u}_2, ..., \overline{u}_8)$.

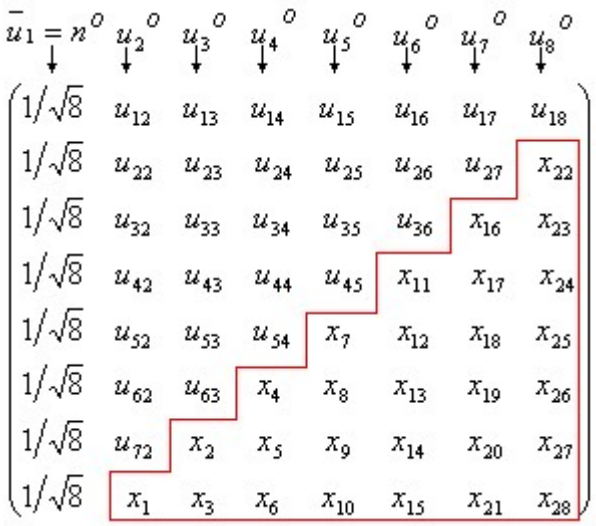


Рис.3.7. Збурена в процесі СПр матриця U

Ефективність СА оцінюється за допомогою коефіцієнта кореляції для ДІ:

$$NC = \left(\sum_{i=1}^{t} p_i' \times \overline{p}_i' \right) \Big/ t ,$$

де $p_i' = 1$, $\overline{p}_i' = 1$, якщо $p_i = 1$, $\overline{p}_i = 1$, и $p_i' = -1$, $\overline{p}_i' = -1$, якщо $p_i = 0$, $\overline{p}_i = 0$ (табл.3.1) .

Таблиця 3.1. Значення *NC* при атаці стиском з різними коефіцієнтами якості на стеганоповідомлення

QF (JPEG)	10	20	25	30	40	50	60	70	75	80	90
NC	0.94	0.95	0.95	0.95	0.95	0.95	0.95	0.96	0.96	0.96	0.96

Питання

1. Що називається контейнером, стеганоповідомленням? Що має сенс використовувати в якості контейнера при організації стеганографічного каналу зв'язку? Чому?
2. Принцип Керхгоффа.
3. Що таке стеганографія, комп'ютерна стеганографія, цифрова стеганографія? Які причини популярності досліджень в області стеганографії в цей час? Класифікація напрямків, які містить у собі стеганографія.
4. Що таке цифровий водяний знак? Для чого він використовується?
5. Структурна схема стеганосистеми.
6. Класифікація стеганосистем.
7. Що таке потоковий, фіксований контейнер?
8. Що представляє із себе обраний, випадковий, нав'язаний контейнер?
9. Яким чином стеганоперетворення можна представити у вигляді елементарних матричних операцій? Пояснити.
10. Вплив норми матриці збурення на процес забезпечення надійності сприйняття стеганоповідомлення.

11. Кількісні різницеві показники надійності сприйняття стеганоповідомлення, їх недоліки.
12. Умови забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера.
13. Чому забезпечення малого значення норми матриці збурення при стеганоперетворенні контейнера є ключовим для забезпечення надійності сприйняття стеганоповідомлення?
14. Відповідність між параметрами двовимірного сигналу в частотній області ЦЗ та областях сингулярного, спектрального розкладання матриці.
15. Яке стеганоповідомлення називається чутливим?
16. Який стеганоалгоритм називається стійким/нестійким до збурних дій?
17. Достатня умова забезпечення малої чутливості СП до збурень.
18. Чим визначається чутливість СП до збурних дій у випадку симетричної матриці?

Тема 4. ГРАФОВО-МАТРИЧНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ СИСТЕМИ, ЗАСНОВАНА НА ПРИНЦИПАХ ФУНКЦІОНУВАННЯ НЕРВОВОЇ СИСТЕМИ ЛЮДИНИ

План

1. Аналогії архітектури та цілей функціонування нервової системи людини та системи захисту інформації
2. Виділення основних принципів та цілей функціонування нервової системи людини
3. Етапи побудови графової моделі захищеної інформаційної системи
4. Метод визначення вагових коефіцієнтів вершин графової моделі системи та зміни їх у процесі функціонування

1. Аналогії архітектури та цілей функціонування нервової системи людини та системи захисту інформації

З кінця минулого століття почав розвиватися «некласичний» підхід у теорії управління, що ґрунтується на аналогіях архітектури та цілей функціонування складних технічних та біологічних систем — природних систем управління, який залишається найперспективнішим на сьогоднішній день. Завдання моделювання людського мозку завжди викликало підвищений інтерес. Практична актуальність створення моделі нервової системи людини (НСЛ) як такої в даний час пов'язана зі зростаючим попитом на системи управління для об'єктів з властивостями, що погано формалізуються. Однак надзвичайна складність об'єкта моделювання та виконуваних ним функцій до теперішнього часу не дає можливості створення досить точної універсальної математичної моделі нервової системи, хоча для цього використовуються такі складні інструменти, як диференціальне та інтегральне числення, методи оптимізації тощо, а також підхід, заснований на створенні штучних нейромереж, який при моделюванні природних систем управління, на жаль, не забезпечує всіх вимог, що висуваються до моделей.

Логіка використання обраної біологічної системи для моделювання ІС випливає з очевидної аналогії між НСЛ та системою інформаційної безпеки (рис.4.1). Слід враховувати, що процес моделювання тут носить комплексний характер і використовує НСЛ, починаючи з форми подання інформації, програмування інформаційних полів і закінчуючи архітектурою ІС із вбудованими механізмами забезпечення інформаційної безпеки та еволюційним перебігом процесів. Моделювання захищених ІС засноване на єдності подання інформації в ієрархії НСЛ, в якій повідомлення передаються універсальним контейнером, що визначається структурованим інформаційним полем ДНК. Структурований характер мають розподілені інформаційні поля нейронних комплексів нервової системи, завдяки яким у НСЛ існують адаптивні механізми пам'яті, що накопичують життєвий досвід. Можливість реалізації адаптивних механізмів пам'яті у штучних інформаційних полях – основна передумова еволюції ІС. Програмування в НСЛ має надлишковий розподілений характер, що забезпечує високу функціональну стійкість інформаційних процесів.

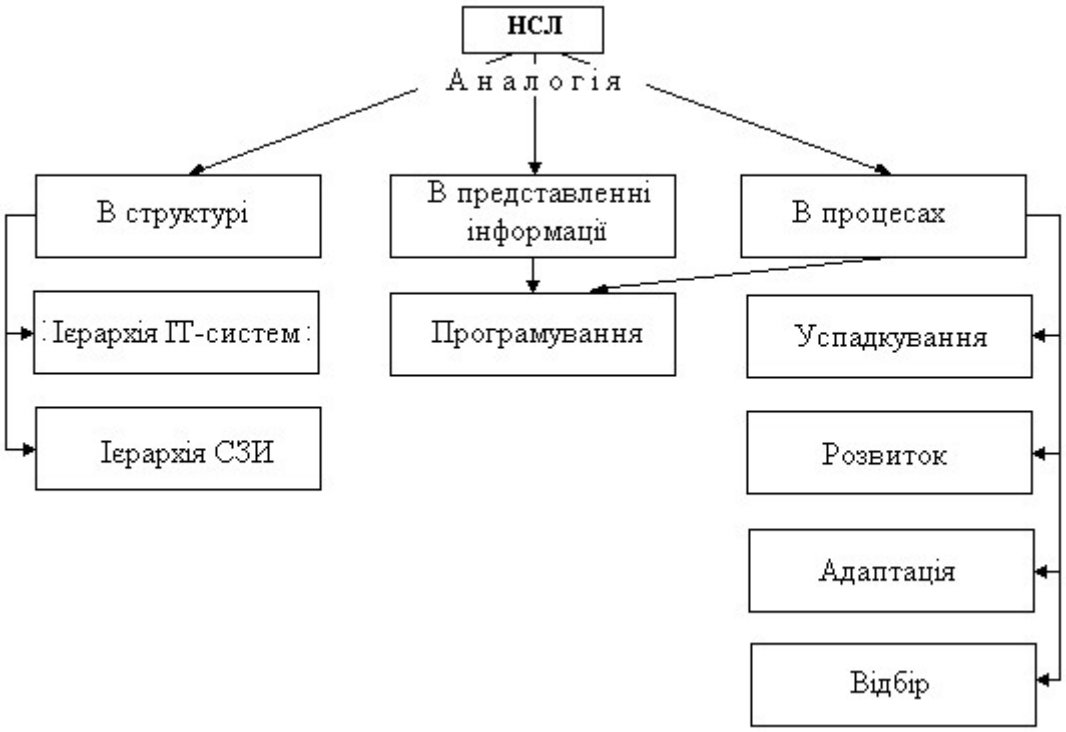


Рис.4.1. Аналогія між нервовою системою людини та системою інформаційної безпеки

Окремі спотворення інформації, з одного боку, компенсуються надмірністю інформаційних полів, а з іншого — дозволяють реалізувати механізм мутацій та еволюційні процеси розвитку та відбору. Зокрема, адаптивні процеси в інформаційних полях дозволяють ІС розвиватися та накопичувати досвід в умовах розширення поля загроз, а успадкування досвіду у подальших реалізаціях системи зводиться до передачі відповідних інформаційних полів. Ієрархія адаптивної системи інформаційної безпеки відображає поділ функцій захисту на керуючу (перевірка форм подання інформації тощо) та керовану, що реалізує взаємодію системи із середовищем. Архітектурною особливістю НСЛ є внутрішній характер механізмів захисту, що реалізується в ієрархії ІС. При моделюванні штучних систем слід враховувати, що при реалізації адаптивних механізмів НСЛ та інформаційних полів її ***функції захисту інформації повинні бути внутрішніми функціями проектованої системи***.

2. Виділення основних принципів та цілей функціонування нервової системи людини

Оскільки відображення в математичному описі всієї сукупності фізіологічних закономірностей і властивостей при обов'язковому обмеженні детальності, специфіки і обсягу характеристик, що включаються в модель, і підсистем не представляється можливим, в першу чергу, необхідно виділити основоположні принципи роботи НСЛ, відповідно до яких буде відбуватися побудова математичної моделі. ***Загальносистемними*** (основними) характеристиками системи назвемо такі властивості та відносини, значення яких у формуванні НСЛ досить виражено. Їх відбір має подолати природне

протиріччя між детальністю (адекватністю) моделі та її ефективністю (конструктивністю) як інструмента дослідження.

Великий вплив на розвиток математичних моделей не тільки НСЧ, а й, наприклад, системи кровообігу та інших, створила концепція поділу системи на ***керуючу і керовану частини***, що використовується нижче. При цьому як керуюча система (КС) в нашій задачі виступає СЗІ, що моделюється з використанням основних принципів функціонування НСЛ, що є складовою сукупної інформаційної системи (ІС) - об'єкта управління (ОУ).

Основні принципи організації та функціонування НСЛ, з урахуванням яких формується модель:

1. *Автономність* - керуюча система є підмножиною об'єкта управління і керує ним на основі знань, отриманих самостійно при взаємодії з навколишнім середовищем за допомогою блоку датчиків (БД) та виконуючого органу;

2. *Дискретність* - як відомо, мозок містить скінченну кількість нейронів, зв'язків і т.д., нервові імпульси людини також дискретні; через це і модель повинна відповідати цим властивостям, тобто КС має зберегти дискретність як структури, так і принципів функціонування;

3. *Максимальна початкова пристосованість* - у реальних умовах процес становлення НСЛ (КС) з метою пристосовуваності до життя у певному середовищі для виживання відбувається під впливом природного відбору. При моделюванні НСЛ природний відбір повинен бути замінений максимальним використанням апріорної інформації. Це використання інформації має відображати наявність пристосованості ОУ та КС до умов функціонування.

4. *Мінімум вхідних даних* - для людини при її народженні властива наявність таких інформаційних просторів, заповнення яких відбувається в ході життя. Аналогічно: КС у момент початку її функціонування містить деякі невизначені властивості, становлення яких відбувається під час накопичення знань під час функціонування системи у реальних умовах.

Основними цільовими функціями КС (нервової системи) є:

- виживання ОУ;
- накопичення знань.

Як відомо з біології, ці дві цільові функції взаємопов'язані між собою в тому сенсі, що досягнення однієї сприяє підвищенню ймовірності досягнення іншої. З огляду на це зосередимо увагу на першій цільовій функції (доцільність вибору цієї функції пояснюється специфікою об'єкта, що є кінцевою метою моделювання: основним для СЗІ є збереження інформації — виживання ОУ).

3. Етапи побудови графової моделі захищеної інформаційної системи

Пригадаємо деякі поняття теорії графів.

Визначення. Граф G - це скінченна непорожня множина V, що містить p вершин, і множина X, що містить q ребер, які представляють з себе пари вершин.

Для неорієнтованого графа ребра являють собою неупорядковані пари вершин з множини V, для орієнтованого графа ребра - це впорядковані пари вершин з V (тобто в орієнтованому графі для кожного ребра важливий напрямок: з якої вершини ребро виходить і в яку вершину входить).

Якщо вершини u і v графа G з'єднані ребром, вони будуть називатися *суміжними* вершинами графа. Ребро, що проходить через вершину, називається *інцидентним* цій вершині.

Якщо два різні ребра інцидентні одній вершині, то вони називаються *суміжними*. Якщо граф містить єдину вершину й не містить ребер, то він називається *тривіальним*.

Ребра, інцидентні одній парі вершин, називаються *кратними.* Граф, що містить кратні ребра, називається *мультиграфом*. Ребро, кінцями якого є співпадаючі вершини, називається *петлею*.

Ступенем вершини $v \in V$ неорієнтованого графа G називається кількість ребер $\rho(v)$, інцидентних вершині v. У неорієнтованому графі сума ступенів усіх вершин дорівнює подвоєному числу ребер графа. Петля в ступінь відповідної вершини дає внесок 2. Якщо вершина має ступінь, що дорівнює 0, вона називається *ізольованою* вершиною графа.

Нехай G - неорієнтований граф.

Маршрутом в графі G називається послідовність $v, \{v,w\}, w, \{w,t\}, t, ..., m, \{m,p\}, p$ вершин і ребер цього графа, яка починається й закінчується вершиною, а кожне ребро послідовності інцидентне двом вершинам, одна з яких безпосередньо передує йому, а інша безпосередньо іде за ним. Зазначений маршрут з'єднує вершини v і p і його можна позначити: $v, w, t, ..., m, p$ (тобто указати послідовність вершин).

Маршрут називається *замкненим*, якщо $v = p$, тобто початкова й кінцева вершини маршруту співпадають.

Маршрут називається *ланцюгом*, якщо всі його ребра різні, *простим ланцюгом*, якщо всі вершини, а отже й ребра, різні. Замкнений ланцюг називається *циклом*. Замкнений простий ланцюг називається *простим циклом*.

Граф, який не містить циклів, називається *ациклічним*. Число ребер маршруту називається його *довжиною*.

Нехай G - неорієнтований граф. Дві вершини v_i і v_j називаються *зв'язаними*, якщо існує маршрут з кінцями у вершинах v_i і v_j.

Граф G називається *зв'язним*, якщо будь-яка пара його вершин зв'язана.

Відстанню між вершинами v_i і v_j неорієнтованого графа G називається мінімальна з довжин ланцюгів, що з'єднують вершини v_i і v_j.

Ексцентриситетом вершини v графа G називається найбільша з відстаней від цієї вершини до будь-якої іншої вершини графа.

Діаметром графа називається максимальна з відстаней між парами його вершин. Діаметр графа дорівнює максимальному ексцентриситету вершин графа.

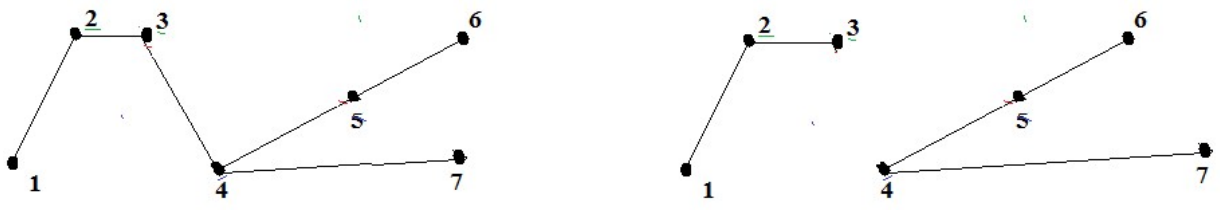
Вузли графа, відстань між якими дорівнює діаметру графа, називаються *периферійними*.

Неорієнтований граф називається *деревом*, якщо він зв'язний і не містить циклів (а тому не містить петель і кратних ребер) (рис.4.2(а)). Дерево - це мінімальний зв'язний граф: при видаленні хоча б одного ребра він втрачає зв'язність.

Дерево з n вершинами має $n-1$ ребро. Усі ребра в дереві є мостами.

Лісом називається незв'язний граф без циклів (рис.4.2(б)). Зв'язні компоненти лісу є деревами.

Вершини дерева, ступінь яких дорівнює одиниці, називаються *листами* (або *висячими вершинами*). На рис.4.2(а) вершини 1, 6, 7 – листи.



а б

Рис.4.2. Приклади ациклічних графів: а – дерево; б – ліс

У дереві будь-які дві вершини зв'язані єдиним ланцюгом.

Коренева структура рівнів (КСР) графа з коренем у вузлі x $\Im(x)$ є розбивка множини вершин V графа:

$$\Im(x) = \{L_0(x), L_1(x), ..., L_{l(x)}(x)\},$$

така, що $L_0(x) = \{x\}, L_1(x) = Adj(L_0(x)), L_i(x) = Adj(L_{i-1}(x)) - L_{i-2}(x), \quad i = 2,3,...,l(x)$, де $Adj(L_{i-1}(x))$ - множина вузлів графа, що не належать $L_{i-1}(x)$, але суміжних хоча б з одним вузлом з $L_{i-1}(x)$. Ексцентриситет $l(x)$ вузла x стосовно структури рівнів називається довжиною $\Im(x)$, а ширина $w(x)$ структури $\Im(x)$ визначається як

$$w(x) = \max\{|L_i(x)| \,|\, 0 \le i \le l(x)\}.$$

Будемо використовувати як модель ОУ зважену графову модель зі структурним співвідношенням «складатися з». Використання такого принципу побудови графа образу об'єкта, яким є ІС, має низку важливих властивостей:

1. Таке структурне співвідношення дає можливість відобразити ієрархію ОУ, автоматично здійснює ієрархічну декомпозицію, необхідну для аналізу СЗІ. Ієрархія - найбільш загальний метод класифікації, який використовується людиною. Така класифікація відтворює первинну форму координації чи організації: 1) коркових процесів, 2) їх психічних співвідносних понять та 3) їх вираз у символах та мовах. Основне завдання в ієрархії, що полягає в оцінці вищих рівнів, виходячи із взаємодії різних рівнів ієрархії, а не безпосередньої залежності від елементів на цих рівнях, збігається з основним завданням при аналізі ІС. Шляхом ієрархічної композиції ухиляються від безпосереднього зіставлення великого і малого. Крім того, ***ієрархічні моделі мають ряд значних переваг*** перед моделями інших видів:
   - дають можливість дослідження «ступеня впливу» пріоритетів на верхніх рівнях на пріоритети елементів нижніх рівнів;
   - надають детальну інформацію про структуру системи;
   - є гнучкими (додавання до добре структурованої ієрархії не руйнують її характеристик).
2. При такому моделюванні КС легко задовольняються основні принципи НСЛ 1, 2:
   - автономність виконується автоматично під час побудови графа; блок датчиків являє собою останній рівень деталізації (сукупність листя графа-дерева), через який відбувається зв'язок із зовнішнім середовищем і всі можливі збурні дії на ІС;
   - дискретність забезпечується властивостями графа як математичного об'єкта: граф – це сукупність двох дискретних скінченних множин вершин і пар вершин (ребер), будь-яке перетворення графа – дискретно;
3. Для такої моделі легко досягти будь-який рівень деталізації, а також модифікації існуючих рівнів деталізації, що є важливою вимогою при створенні моделі будь-якої фізіологічної системи, т.к. апріорі, до отримання моделі, найчастіше неможливо визначитися з тим, наскільки «детальною» має бути модель:

- більша деталізація досягатиметься впровадженням нового рівня листів у вже наявному графі;
- при надмірній наявній деталізації її зменшення еквівалентно побудові гомоморфної згортки підграфа, що містить листя, що відповідають «нецікавим» зараз деталям, і вершини попереднього рівня кореневої структури графа, суміжної зі згаданим листям;

4. Будь-яка модифікація КС зведеться до зміни структури суміжності відповідного підграфа. На даний момент розроблено різні схеми зберігання графа, застосування яких дозволяє проводити обробку графів, зокрема модифікацію структури суміжності, використовуючи для цього досить малу кількість арифметичних операцій.

Перейдемо безпосередньо до побудови зваженого графа-моделі ІС, що представляє дерево.

Eman 1. ІС в цілому (корінь графа-дерева) розглядається як ізольована вершина (рис.4.3), підграф, що відповідає СЗІ, існує ізольовано, ще не маючи зв'язку з інформацією, що циркулює в системі. СЗІ представляється у вигляді сукупності засобів, що входять до неї як складові частини, кожній з яких відповідає вершина графа, що лежить в другому рівні кореневої структури (рис.4.4 - всі вершини позначені натуральними числами від 1 до *n*). Кожен наступний рівень кореневої структури є наступним рівнем деталізації. Раціональний ступінь детальності визначається допустимими класами збурень та керуючих впливів.

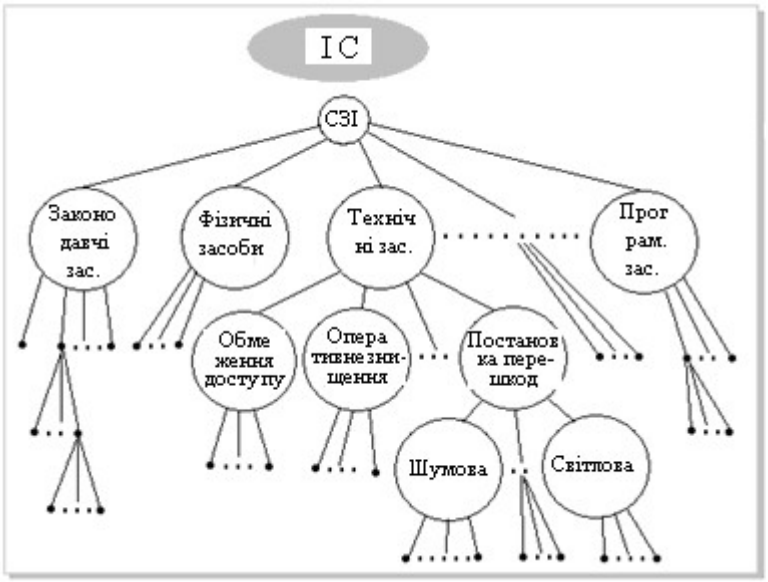


Рис.4.3. Первісний вигляд графа системи

Значення вагових коефіцієнтів графа повинні відображати реальну цінність того чи іншого засобу захисту для функціонування всієї ІС. Конкретні значення коефіцієнтів ґрунтуються на практичному досвіді при максимальному використанні апріорної інформації для забезпечення умови максимальної початкової пристосованості, забезпечують додатну напіввизначеність (додатну визначеність) матриці суміжності графа.

Етап 2. Побудова матриці суміжності MS зваженого графа-моделі, яка в силу його неорієнтованості є симетричною. За допомого нормального спектрального розкладання однозначно визначається спектр і власні вектори MS.

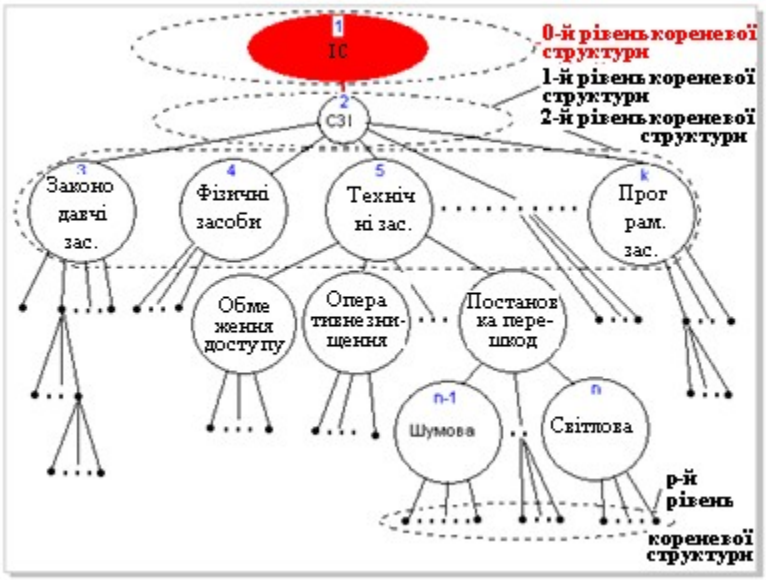


Рис.4.4. Коренева структура рівнів графа системи

Етап 3. Введення зв'язку (ребра) {1,2} (рис.4.4) — інформація, що підлягає захисту, стає доступною для СЗІ, вводиться до цієї системи. Це збурить MS (в результаті отримується матриця $\overline{MS}$), а тому і її власні значення і власні вектори. Сукупність цих збурень є математичним представленням для циркулюючої у системі інформації та не лише для неї (встановлення зв'язку між сукупною ІС та СЗІ відкриває доступ до СЗІ не тільки для інформації, але й для всіх складових ІС, які відсутні безпосередньо у СЗІ). У загальному випадку інформація представляється деякою підмножиною множини збурень власних значень і власних векторів матриці MS.

Спілкування ІС, що моделюється, з навколишнім середовищем здійснюється через блок датчиків-листів (периферична нервова система). Будемо вважати, що всі атаки на систему виражаються у впливі на листя, вагові коефіцієнти яких малі в порівнянні з коефіцієнтами, що відповідають вершинам, що знаходяться на попередніх рівнях кореневої структури. Вага вершини на кожному рівні визначається як додатне число, яке є більшим чи рівним сумі ваг суміжних із нею вершин, що знаходяться на наступному по порядку рівні кореневої структури (рис.4.5 — всередині вузла — його вага, поруч із вузлом — номер).

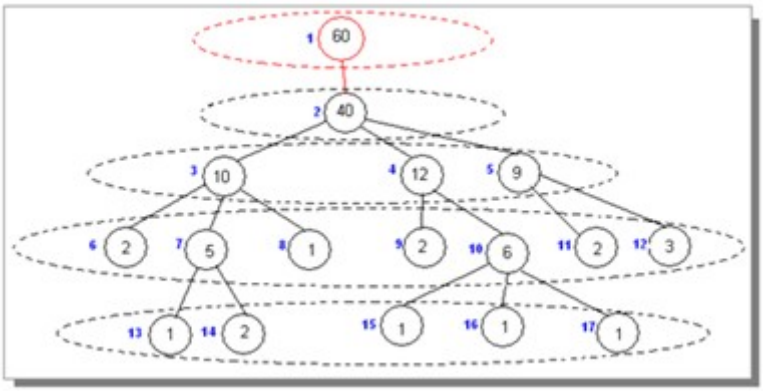


Рис.4.5. Приклад зваженого графа ІС

Математичним виразом атаки буде зменшення вагових коефіцієнтів, що відповідають атакованим засобам захисту.

Введення інформації в систему збурює всі або деякі власні значення (ВЗ) та власні вектори (ВВ) матриці суміжності MS графа-моделі.

Твердження. Зміни в інформації, що зберігається, подаються у вигляді збурень тих ВЗ і ВВ матриці $\overline{MS}$, які збурилися під час введення інформації у систему. Аналіз стану інформації зводиться до аналізу збурень згаданих ВЗ та ВВ.

Оскільки матриця $\overline{MS}$ симетрична, то для аналізу ступеня руйнування (збереження) інформації віддамо перевагу аналізу збурень її спектра (ВЗ), оскільки він містить лише добре обумовлені ВЗ. Добра обумовленість ВЗ призводить до нечутливості всього спектра симетричної матриці $\overline{MS}$ до збурних дій або, інакше кажучи, до того, що збурення ВЗ по абсолютній величині можна порівняти з величиною самої збурної дії, чого не можна в загальному випадку сказати про ВВ (їх чутливість в межах матриці залежить від абсолютної відокремленості відповідних ВЗ). Чутливі ВВ можуть відхилитися на великий кут при малій збурній дії (навіть через округлення, що відбуваються при обчисленнях), і тим самим їх збурення не дають істинної інформації про величину збурної дії (про серйозність атаки). Про величину збурної дії (або серйозності атаки) можна судити лише по ВВ, що відповідають ВЗ з найбільшими абсолютними відокремленнями.

4. Метод визначення вагових коефіцієнтів вершин графової моделі системи та зміни їх у процесі функціонування

При прийнятому підході до розв'язання задачі про моделювання ІС важливу роль відіграють вагові коефіцієнти вершин графа-моделі, які відповідають елементам системи. Значення вагових коефіцієнтів мають чисельно відбивати реальну значимість будь-якого засобу захисту (чи групи засобів) для функціонування СЗІ загалом, попри їхню відмінність (технічні, законодавчі, програмні і т.д. засоби). Для забезпечення одного з основних принципів функціонування НСЛ, максимальної початкової пристосованості, вагові коефіцієнти повинні бути отримані, виходячи з практичного досвіду при максимальному використанні апріорної інформації. До сьогодні питання кількісної оцінки захищеності об'єктів, ефективності засобів захисту інформації, можливостей противника, а також методики для таких оцінок

опрацьовані недостатньо. Для визначення вагових коефіцієнтів вузлів, що відповідають технічним засобам захисту, запропоновані деяки методи. Задача визначення конкретних числових значень інших вагових коефіцієнтів досі залишалася невирішеною.

Використовуючи визначення ієрархії, дане в попередніх лекціях, будемо вважати, що елементи в кожній групі (рівні) ієрархії незалежні.

Запропонована модель ІС представляє ієрархію, для якої $L_1 = \{s\}$, де s відповідає сукупній ІС, а кожний рівень ієрархії L_k є одночасно і рівнем кореневої структури графа-моделі (рис.4.6, порівн. з рис.4.4).

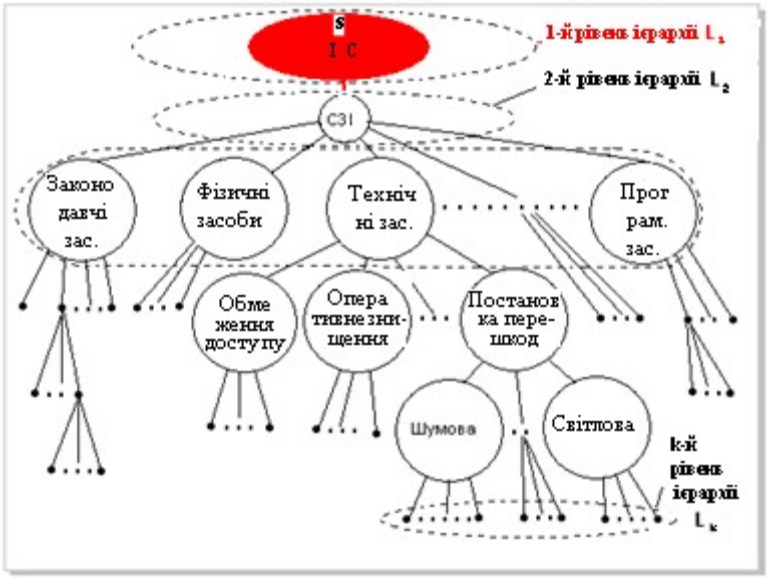


Рис.4.6. Структура рівней ієрархії моделі системи

Ієрархія є певний тип системи, заснований на припущенні, що елементи системи можуть групуватися в незв'язані множини. Елементи кожної групи знаходяться під впливом елементів деякої цілком визначеної групи і, у свою чергу, впливають на елементи іншої групи. Вважаємо, що елементи в кожній групі ієрархії (що називається рівнем, кластером) незалежні.

Наступний приклад зробить поняття ієрархії зрозумілішим. Нехай ми прагнемо визначити сценарій, згідно з яким із найбільшою ймовірністю буде забезпечено тривале існування коледжу. Назвемо добробут коледжу *загальною метою*. На неї впливають такі *сили*: навчання, громадське життя, дух (атмосфера), наявність обладнання та позашкільна діяльність. Ці сили визначаються такими *акторами* (*дійовими особами*): академічною адміністрацією, неакадемічною адміністрацією, професорсько-викладацьким складом, студентами, попечителями. Ми опускаємо очевидний зворотний зв'язок між силами та акторами. Різні актори мають певні *цілі*: професорсько-викладацький склад може хотіти зберегти свою роботу, зростати професійно, якісно проводити навчання; студенти можуть бути зацікавлені в отриманні роботи, одруженні, в отриманні хорошої освіти і т. д. Нарешті, є кілька можливих *сценаріїв*, таких як: статус-кво, наголос на професійне навчання, подальшу освіту або перетворення на релігійну школу. Сценарії визначають можливість досягнення цілей, цілі впливають на акторів, актори спрямовують

сили, які, нарешті, впливають на добробут коледжу. Отже, ми отримуємо ієрархію (рис. 4.7).

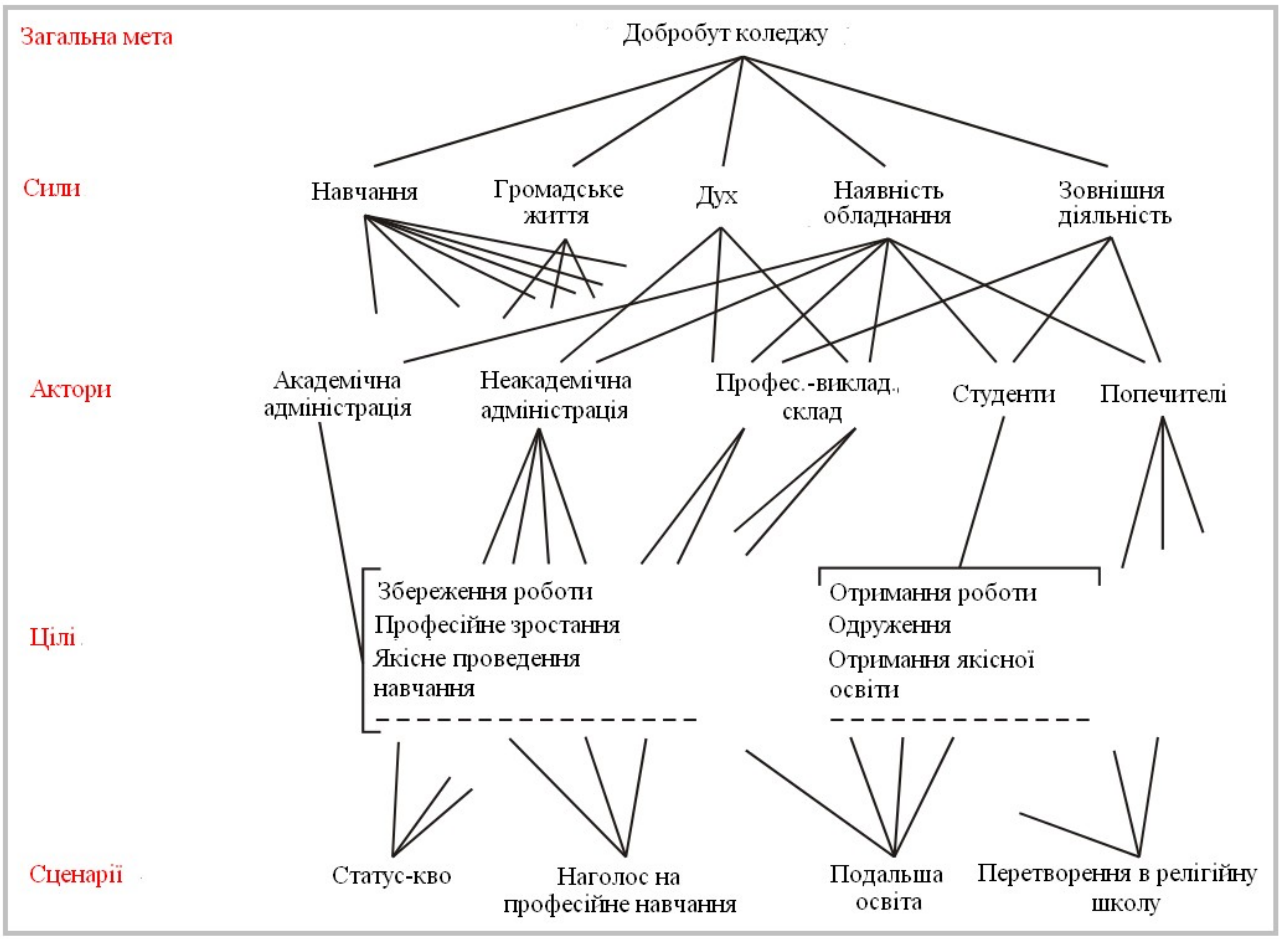


Рис.4.7. Приклад ієрархії

Центральним питанням мовою ієрархії є таке: наскільки сильно впливають чинники найнижчого рівня ієрархії на вершину – загальну мету? Нерівномірність впливу з усіх чинників призводить до необхідності визначення інтенсивності впливу, чи пріоритетів чинників. Визначення пріоритетів факторів нижчого рівня щодо мети може бути зведено до послідовності завдань визначення пріоритетів для кожного рівня, а кожне таке завдання – до послідовності попарних порівнянь. Порівняння залишаються основними складовими цієї теорії.

Ієрархії стійкі та гнучкі; вони стійкі в тому сенсі, що малі зміни викликають малий ефект, а гнучкі в тому сенсі, що додавання до добре структурованої ієрархії не руйнують її характеристик.

При побудові ієрархічної структури системи виникають два питання:

- Як ми будуємо функції ієрархічно?
- Як ми вимірюємо вплив будь-якого елемента в ієрархії?

На практиці немає встановленої процедури генерування цілей, критеріїв та видів діяльності для включення до ієрархії або навіть у більш загальну систему. Це залежить від тих цілей, які ми вибираємо для декомпозиції складної системи. Зазвичай ця процедура починається з вивчення літератури для

збагачення думками, і часто, знайомлячись з чужими роботами, ми проходимо через стадію мозкового штурму для складання переліку всіх концепцій, суттєвих для завдання, незалежно від їхнього співвідношення чи порядку. Слід пам'ятати, що основні цілі встановлюються на вершині ієрархії; їх підцілі – безпосередньо нижче вершини; сили, що обмежують діючих осіб, ще нижче. Сили домінують над рівнем самих діючих осіб, які, у свою чергу, домінують над рівнем своїх цілей, нижче за які буде рівень їх можливих дій, і в самому низу знаходиться рівень різних можливих результатів (сценаріїв). Це природна форма, яку приймають ієрархії, пов'язані з плануванням та конфліктами. В ієрархії, призначеної для фізичної системи, можливі дії можуть бути замінені методами конструювання. За ними повинні йти кілька проміжних рівнів. Перш ніж буде сформовано добре визначений план, можуть знадобитися значні критичні зауваження та повторної перевірки.

Нам потрібний метод визначення сили, з якою різні елементи одного рівня впливають на елементи попереднього рівня, щоб можна було обчислювати величину впливів елементів найнижчого рівня на загальну мету.

Для більшої ясності повернемося до ієрархії колледжу (рис.4.7). Нас цікавить «сценарій, за яким із найбільшою ймовірністю буде забезпечено тривале існування коледжу». Для визначення цього сценарію спочатку знаходимо важливість сил щодо спільної мети. Потім для кожної сили визначаємо ступінь впливу акторів на цю силу. Звідси нескладним обчисленням отримуємо ступінь впливу акторів на спільну мету. Потім оцінюємо важливість цілей для кожного актора і нарешті визначаємо дієвість різних сценаріїв у забезпеченні досягнення кожної мети. Повторивши кілька разів згадані вище обчислення отримаємо «найкращий» сценарій.

Всі описані вище дії виконує метод аналізу ієрархій (MAI), який можна описати в такий спосіб. Припустимо, що задані елементи одного, скажімо, четвертого рівня ієрархії та один елемент I наступного вищого рівня. Потрібно порівняти елементи четвертого рівня попарно за силою їх впливу на I, помістити числа, що відображають досягнуту при порівнянні згоду в думках, в матрицю і знайти власний вектор, що відповідає найбільшому власному значенню. Власний вектор забезпечить впорядкування пріоритетів, а власне значення буде мірою узгодженості суджень.

Для більшого розуміння дій, що передбачаються MAI, визначимо шкалу пріоритетів для дуже простого прикладу. Нехай A, B, C та D позначають стільці, розставлені по прямій лінії, що веде від джерела світла. Створимо шкалу пріоритетів відносної освітленості для стільців. Судження робить людина, що стоїть біля джерела світла, у якого запитують: «Наскільки сильніша освітленість стільця B порівняно з C?» Він відповідає одним із чисел для порівняння, записаних у таблиці, і ця думка заноситься в позицію (B, C) матриці:

Освітленість	A	B	C	D
A				
B				
C				
D				

За згодою порівняння сили завжди проводиться для дії або об'єкта, що стоїть у лівому стовпці, стосовно дії або об'єкта, що стоїть у верхньому рядку. Ми маємо *матрицю попарних порівнянь* для чотирьох рядків та чотирьох стовпців (матриця 4x4).

Домовимося, що це такі числа. Нехай задані елементи А та В; якщо:

• А та В однаково важливі, заносимо 1;

• А трохи важливіше, ніж В, заносимо 3;

• А значно важливіше В, заносимо 5;

• А явно важливіше В, заносимо 7;

• А за своєю значимістю абсолютно перевершує В, заносимо 9 у позицію (А, В), де перетинаються рядок А та стовпець В.

При порівнянні елемента із самим собою маємо рівну значущість, так що на перетині рядка А зі стовпцем А у позиції (А, А) заносимо 1. Тому головна діагональ матриці має складатися з одиниць. Заносимо відповідні зворотні величини: 1, 1/3, ..., або 1/9 на перетинах стовпця А і рядка В, тобто в позицію (В, А) для порівняння В з А. Числа 2, 4, 6, 8 та їх зворотні величини можуть використовуватися для полегшення компромісів між судженнями, що злегка відрізняються від основних чисел. Отримуємо додатну зворотно-симетричну матрицю. Формально досягнення узгодженості суджень буде еквівалентно вимозі рівності максимального власного значення λ_{max} отриманої матриці її розміру n: $\lambda_{max} = n$. Відхилення від узгодженості також можна оцінити за допомогою: $\frac{\lambda_{max} - n}{n-1}$. Це значення називається *індексом узгодженості* (ІУ). Індекс узгодженості згенерованої випадковим чином за шкалою від 1 до 9 зворотно-симетричної матриці з відповідними оберненими величинами елементів, називається *випадковим індексом* (ВІ). Нижче наведені порядок матриці (перший рядок) і середні значення ВІ (другий рядок):

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0.58	0.9	1.12	1.24	1.32	1.41	1.45	1.49	1.51	1.48	1.56	1.57	1.59

У матриці для нашого прикладу зі стільцями є 16 полів. Чотири з них визначені: на головній діагоналі – одиниці. Для 12 чисел, що залишилися після заповнення діагоналі, потрібно провести шість порівнянь, оскільки інші шість є зворотними порівняннями і їх оцінки повинні бути зворотними величинами до оцінок перших шести. Припустимо, що людина, використовуючи рекомендовану шкалу, вносить число 4 в позицію (В, С), оскільки вважає, що інтенсивність освітленості стільця В порівняно зі стільцем С знаходиться між слабкою і сильною. Тоді в позицію (С, В) автоматично заноситься обернена величина, тобто 1/4. Після проведення п'яти суджень, що залишилися, а також занесення їх зворотних величин, для всієї матриці отримаємо:

Освітленість	A	B	C	D
A	1	5	6	7
B	1/5	1	4	6
C	1/6	1/4	1	4
D	1/7	1/6	1/4	1

Тут $\lambda_{max} = 4.3907$.

Наступний крок полягає у обчисленні вектора пріоритетів за даною матрицею. У математичних термінах це - обчислення головного власного вектора, тобто власного вектора, що відповідає максимальному власному значенню, який після нормалізації стає вектором пріоритетів:

$$U_1 = \begin{pmatrix} 0.9219 \\ 0.3507 \\ 0.1504 \\ 0.0672 \end{pmatrix}.$$

Для досягнення поставленої мети визначимо пріоритети елементів кожного рівня ієрархії L_k по відношенню до s, тобто чисельно відобразимо значимість будь-якого засобу захисту (чи сукупності засобів) для функціонування системи загалом, використовуючи при цьому метод аналізу ієрархій (MAI) з урахуванням особливостей побудованої ієрархічної моделі.

MAI виник у результаті розробки методології для моделювання неструктурованих, погано формалізованих задач в економіці, теорії управління, параметри яких не піддаються ефективним кількісним оцінкам. Він широко використовується і добре зарекомендував себе при вирішенні різних задач не тільки економіки, а й теорії дослідження операцій, при аналізі ризиків, при побудові експертних систем та в багатьох інших областях. Математична правомочність MAI базується на методі власного значення та принципі ієрархічної композиції, що мають чітке математичне обґрунтування. Однак вхідна інформація в методі, що розглядається, надходить як інформація від експертів. І хоча MAI має можливість перевірки експертної інформації на несуперечність за допомогою індексу узгодженості, це не вирішує всіх проблем, пов'язаних з використанням експертних оцінок. Дійсно, при «незадовільному» значенні індексу узгодженості потрібне коригування вхідних даних з наступним перерахуванням результатів отриманих пріоритетів, що тягне за собою чималі додаткові обчислювальні витрати. З іншого боку, можливості експертів давати несуперечливу інформацію зі збільшенням кількості параметрів задачі обмежені. Виходячи з вищесказаного, при використанні MAI для побудови моделі ІС, а саме, для визначення значення вагових коефіцієнтів вузлів графа системи, бажано зменшити вплив суб'єктивізму на вхідну інформацію шляхом використання не експертних оцінок, а статистичних даних. Для цього може використовуватися наступна процедура.

Перший крок полягатиме у накопиченні статистичних даних про роботу ІС. Нехай аналіз системи проводиться протягом часу T. Передбачається, що набір елементів, що входять до системи, за час T не змінюється. Нехай x_j відповідає конкретному засобу захисту, якому в графовій моделі відповідає вершина-лист. Серед наявних у розпорядженні системи засобів захисту є постійно діючі, а також такі, що підключаються при виявленні спроби нападу. Назвемо *позитивним результатом роботи* x_j ситуацію, коли активація даного засобу (у випадку, коли x_j належить до другої групи) або його неперервна робота (коли x_j належить до першої групи) призводить до запобігання несанкціонованому доступу. Кількість усіх позитивних результатів роботи x_j за час T позначимо $k(x_j)$. Назвемо *коефіцієнтом ефективної роботи* (КЕР) $f(x_j)$ засобу x_j відношення $f(x_j)=\dfrac{k(x_j)}{K}$, де K — загальна кількість спроб несанкціонованого доступу до системи за час T.

Статистичні дані накопичуються як для окремих засобів захисту, так і для їх сукупностей, в які ці засоби логічно об'єднані при побудові графа (їм відповідають вершини графа, які не є листями). Наприклад, припустимо, що несанкціонований доступ запобігли завдяки шумовій перешкоді. При збиранні статистичних даних такий випадок призведе до збільшення на одиницю кількості позитивних результатів роботи безпосередньо засобу "шумова перешкода", сукупностей "постановка перешкод", "технічні засоби захисту" тощо. (див. рис.4.6). КЕР для сукупностей засобів захисту будуть визначатися аналогічно тому, як це було запропоновано вище для x_j. Зауважимо, що якщо $y_j \in L_k$ відображає деяку сукупність засобів, представлених на наступному рівні ієрархії (кореневої структури) L_{k+1}, що позначаються як $x_1, x_2, ..., x_n$, то в загальному випадку

$$k(y_j) \geq \sum_{i=1}^{n} k(x_i),\ f(y_j) \geq \sum_{i=1}^{n} f(x_i), \qquad (4.1)$$

де $k(y_j)$ і $f(y_j)$ — відповідно кількості позитивних результатів спрацьовувань та КЕР для сукупності y_j. Знаки нерівностей у співвідношеннях (4.1) пояснюються тим, що при побудові математичної моделі ІС неможливо врахувати всі чинники, що впливають на її функціонування. Можливо, що у реальній системі до складу y_j входить крім засобів $x_1, x_2, ..., x_n$ ще й x_0, значимість якого настільки мала, що при побудові моделі він не був врахований окремо.

Збір статистичних даних необов'язково проводити по аналізу реальних атак на систему. При моделюванні будь-якої СЗІ необхідно, щоб вона виявилася стійкою по відношенню до передбачуваних атак. В силу цього будемо вважати, що набір $\{V_1, V_2, ..., V_l\}$ можливих атак та статистика їх застосування відомі. Моделюючи фізично ці атаки, частково чи повністю штучно «виводячи з ладу» той засіб захисту, куди спрямована атака, проводиться збір необхідних даних, описаних вище.

Такий спосіб збору статистик дає можливість розширити набір характеристик роботи системи. Нехай атака V_j спрямована безпосередньо на засіб x_i. Приведемо штучно систему у стан, що відповідає результату атаки V_j. Цю модифіковану систему замість вхідної використовуємо для накопичення кількості позитивних результатів роботи її елементів, як було запропоновано вище. Зробимо це для кожної можливої атаки V_j. Нехай $x_1, x_2, ..., x_p$ — вся множина засобів захисту аналізованої системи (множина листів в графі-моделі). Складемо матрицю S:

	x_1	x_2	$\cdots$	x_p
V_1	$k_{V_1}(x_1)$	$k_{V_1}(x_2)$	$\cdots$	$k_{V_1}(x_p)$
V_2	$k_{V_2}(x_1)$	$k_{V_2}(x_2)$	$\cdots$	$k_{V_2}(x_p)$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
V_l	$k_{V_l}(x_1)$	$k_{V_l}(x_2)$	$\cdots$	$k_{V_l}(x_p)$

де $k_{V_j}(x_m)$ — кількість позитивних результатів роботи засобу x_m в системі, яка зазнала попередньо атаку V_j. Якщо атака V_j повністю зруйнувала засіб x_i, на який була спрямована, то $k_{V_j}(x_i) = 0$. По матриці S очевидно визначається матриця КЕР для описаних випадків модифікації системи.

Використання КЕР як вагових коефіцієнтів для відповідних вершин графа-моделі, яке, на перший погляд, здається можливим, є небажаним. Специфіка графово-матричної моделі системи, що ґрунтується на принципах роботи НСЛ, така, що числові значення вагових коефіцієнтів повинні якомога точніше відповідати реальній значущості кожного засобу або сукупності засобів для функціонування системи, а статистичні оцінки досить точні лише на дуже великих вибірках. Якщо проміжок часу T виявиться недостатньо довгим, то значення $f(x_j)$ можуть сильно відрізнятися від реальних значень. Однак загальна тенденція порівняльної значущості різних засобів захисту по відношенню один до одного для запобігання несанкціонованому доступу проявиться навіть тоді, коли значення T порівняно невелике.

Другий крок. Для оцінки дії різних компонент на всю ІС і обчислення пріоритетів цих компонент скористаємося МАІ.

Функцію w_x, що фігурує в визначенні ієрархії, можна однаково визначити для всіх L_k, прирівнюючи її до нуля для тих елементів в L_{k+1}, які не належать x^-.

Очевидно, кількість рівнів ієрархії графа-моделі ІС більша за два.

Нехай $x_1, x_2, ..., x_n$ — елементи одного рівня ієрархії. Спочатку ваги вершин $w_1, w_2, ..., w_n$ визначаються впливом (пріоритетом) $x_1, x_2, ..., x_n$ на суміжний з ними елемент y_j попереднього рівня. Для цього формується матриця A розміром $n \times n$ парних порівнянь впливу $x_1, x_2, ..., x_n$ на y_j, для чого використовуються отримані на першому кроці КЕР.

Елементи a_{ij} матриці A визначаються за наступним правилом з використанням шкали $\{1,2,...,9\}$:

$$a_{ij}=\begin{cases}1,\ якщо\ f_i\ і\ f_j\ мають\ однакові\ значення\\ 3, якщо\ f_i\ незначно\ більше\ f_j\\ \frac{1}{3}, якщо\ f_j\ незначно\ більше\ f_i\\ 5, якщо\ f_i\ значно\ більше\ f_j\\ \frac{1}{5}, якщо\ f_j\ значно\ більше\ f_i\\ 7, якщо\ f_i\ явно\ більше\ f_j\\ \frac{1}{7}, якщо\ f_j\ явно\ більше\ f_i\\ 9,\ якщо\ f_i\ абсолютно\ перевищує\ f_j\\ \frac{1}{9},\ якщо\ f_j\ абсолютно\ перевищує\ f_i\end{cases}, \quad i,j=\overline{1,n}.$$

Матриця A буде узгодженою ($\lambda_{\max}=n$), якщо $a_{ik}=a_{ij}a_{jk}$, $i,j,k=\overline{1,n}$. Відповідний λ_{max} власний вектор забезпечує впорядкування пріоритетів.

Встановимо тепер пріоритет кожного елемента побудованої ієрархічної моделі ІС щодо головної мети системи в цілому. Іншими словами, визначимо пріоритети (вагові коефіцієнти) для вершин будь-якого рівня кореневої структури графа-моделі щодо вершини $s=L_1$, що є максимальним елементом ієрархії (коренем дерева).

Третій крок. Нехай $Y=\{y_1,...,y_{m_k}\}\subseteq L_k$, а $X=\{x_1,...,x_{m_{k+1}}\}\subseteq L_{k+1}$. Не обмежуючи спільності міркувань, можна припустити, що $Y=L_k$, $X=L_{k+1}$. Нехай елемент $z\in L_{k-1}$, такий, що будь-який елемент множини Y належить множині z^-. Для кожного елемента $x_i, i=\overline{1,m_{k+1}}$ визначений пріоритет цього елемента $w_{y_j}(x_i)$ по відношенню до кожного елемента y_j, $j=\overline{1,m_k}$ попереднього рівня. Для кожного елемента y_j з рівня ієрархії L_k визначений його пріоритет $w_z(y_j)$ відносно $z\in L_{k-1}$ (рис.4.8). Якщо через w позначити функцію пріоритета елементів з X відносно z, то

$$w(x_i)=\sum_{j=1}^{m_k} w_{y_j}(x_i)w_z(y_j),\ i=\overline{1,m_{k+1}}. \qquad (4.2)$$

Співвідношення (4.2), по суті, є процесом зважування пріоритетів x_i відносно елементів y_j за допомогою пріоритетів y_j відносно z.

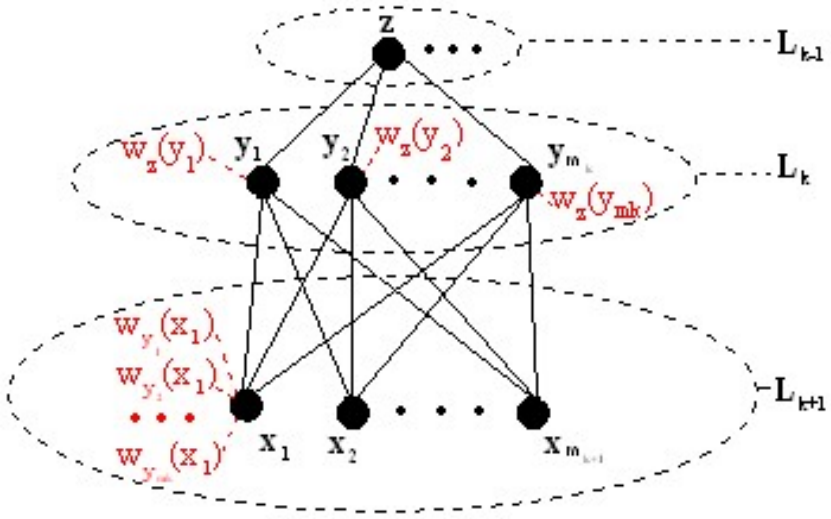


Рис.4.8. Послідовне визначення пріоритетів елементів ієрархії

Очевидно, процес послідовного обчислення пріоритетів $\{x_1,...,x_{m_{k+1}}\} = L_{k+1}$ можна продовжити по індукції відносно елементів рівней $L_{k-2},...,L_1$, цим визначаючи пріоритети будь-якого елемента ієрархії щодо головної мети L_1.

Для графової моделі ІС, що розглядається, перерахунок пріоритетів за формулою (4.2) вимагає незначних обчислювальних витрат: кожен елемент $\{x_1,...,x_{m_{k+1}}\} = L_{k+1}$ матиме ненульове значення пріоритету лише по відношенню до одного елемента y_j попереднього рівня L_k (рис.4.9). Тоді формула (4.2) для перерахунку пріоритетів набуде вигляду:

$$w(x_i) = w_{y_j}(x_i) w_z(y_j),\ i = \overline{1, m_{k+1}},$$

де y_j — це єдиний елемент попереднього рівня ієрархії, для якого $w_{y_j}(x_i) \neq 0$. Таким чином, для того, щоб обчислити пріоритет деякого елемента x_i побудованої ієрархічної графової моделі СЗІ щодо його впливу на систему в цілому необхідно перемножити пріоритети вузлів простого ланцюга, що з'єднує x_i з s (рис.4.9).

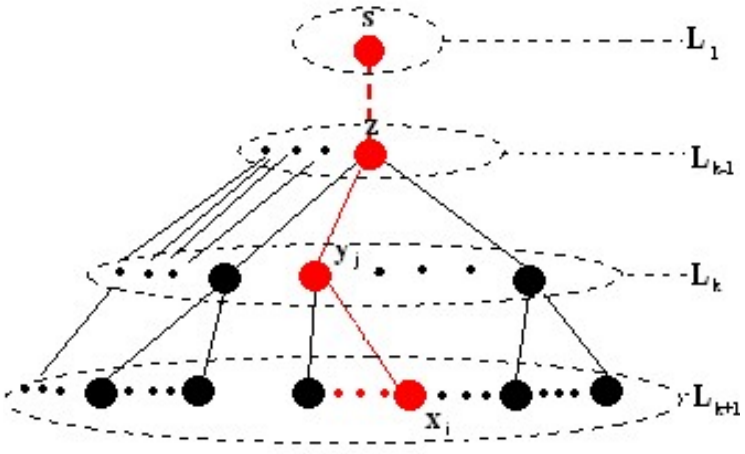


Рис.4.9. Ланцюг впливу елементу x_i на максимальний елемент ієрархії ІС

Питання.

1. В чому полягає аналогія архітектури та цілей функціонування нервової системи людини та системи захисту інформації?
2. В чому полягає автономність керуючої системи?
3. Як розуміється дискретність керуючої системи?
4. Що означає максимальна початкова пристосованість керуючої системи?
5. Що передбачає принцип мінімуму вхідних даних для керуючої системи?
6. Основні цільові функції керуючої системи.
7. Переваги ієрархічних моделей.
8. Яким є структурне співвідношення зваженої графової моделі ІС? Які властивості надає таке структурне співвідношення відповідній моделі?
9. Етапи побудови зваженого графа-моделі ІС.
10. Як формально визначаються зміни в інформації, що зберігається в ІС?

Література

Базова

1. М.М.Браіловський, С.В.Зибін, А.А.Кобозєва, В.О.Хорошко, Ю.Є.Хохлачова. Аналіз кіберзахищеності інформаційних систем. – К.: ФОП Ямчинський О.В., 2021. – 360 с.
2. Кобозєва А.А., Хорошко В.О. Аналіз захищеності інформаційних систем. - К.: Вид. ДУІКТ, 2010. – 316 с.
3. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних підручник. / Г.Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. – Київ: «Центр учбової літератури», 2018. –558 с.
4. Steganography - The Art of Hiding Information: The Art of Hiding Information. - BoD – Books on Demand, 2024. 160 p.
5. Abid Yahya. Steganography Techniques for Digital Images. Springer, 2018. – 122 p.

Допоміжна

1. Bobok I.I., Kobozeva A.A. Steganalysis method efficient for the hidden communication channel with low capacity. *Радіотехніка*. 2019. 198. С. 19–31.
2. Kobozieva at al. Method for Estimating the Bandwidth Capacity of a Steganographic Communication Channel/ PROBLEMELE ENERGETICII REGIONALE. 2(66). 2025. Pp.90-104
3. Кобозєва А.А., Бобок І.І. Локалізація області збурень формальних параметрів стеганографічного контейнера для забезпечення стійкості стеганосистеми/ Вісті вищих учбових закладів. Радіоелектроніка. Т.67, № 8, с.
4. Кобозєва А.А., Бобок І.І. Стеганоаналітичний метод виявлення LSB-вкладень в цифровому відео, послідовності цифрових зображень / Обробка інформації в системах управління та прийняття рішень. Проблеми та рішення. Монографія / Аксак Н., Бобок І. і др.; під наук. ред. проф. В.Вичужаніна – Одеса: НУ «ОМА», 2023 – 358 с.
5. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. Radiotekhnika. 2021. 4(207). P. 27–39.

Інтернет ресурси

1. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
2. Gloe T., Böhme R. The "Dresden Image Database" for benchmarking digital image forensics. *Proceedings of the 2010 ACM Symposium on Applied Computing (SAC '10)*. New York, 2010. P. 1585–1591. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.225.4857&rep=rep1&type=pdf
3. Hsu Y., Chang S. Detecting image splicing using geometry invariants and camera characteristics consistency. *2006 IEEE International Conference on Multimedia and Expo*, Toronto, 2006. P. 549–552. https://www.ee.columbia.edu/ln/dvmm/publications/06/hsu06ICMEcrf.pdf

4. Library of Hadamard Matrices [Electronic resource], https://documents.uow.edu.au/~jennie/hadamard.html
5. MatLAB documentation [Electronic resource], https://uk.mathworks.com/help/matlab/