УДК 004.681:681.326

д.т.н., проф. **Хорошко В.А.** (ДУИКТ)
к.т.н., доц. **Казаков Н.Ф.** (ДУИКТ)
Сирченко Г.А. (ДУИКТ)
Тискина Е.О. (ДУИКТ)

ВЫДЕЛЕНИЕ ОПТИМАЛЬНОЙ СОВОКУПНОСТИ ПОДПРОГРАММ ИЗ ОСНОВНОЙ ПРОГРАММЫ РАБОТЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Рассматриваются вопросы выделения полного множества подпрограмм. Предлагается алгоритм решения задачи оптимизации.
Ключові слова: защита інформації,задача оптимизации.

Рассматриваются вопросы выделения полного множества подпрограмм. Предлагается алгоритм решения задачи оптимизации.
Ключевые слова: защита информации, задача оптимизации.

Questions of allocation of full set of subroutines are considered. The algorithm of the decision of a problem of optimisation is offered.
Keywords: information protection, optimisation problem

Введение. При проектировании систем защиты информации (СЗИ) важное место занимает задача оптимального выбора управляющих автоматов (УА) подсистем защиты, структура которого зависит от программы работы всей СЗИ и центрального компьютера системы. Будем считать, что программа работы СЗИ L представляется последовательностью операторов $a_i \in A; i = 1 \div M$ (строкой операторов). Известно, что некоторому подмножеству операторов $A_i \subset A$ может соответствовать одна операция $O_\xi \in O$, $\xi = 1 \div Z$.

Таким образом, операторы в программе могут быть одинаковыми по выполняемой операции, но всегда понимаются различными, так как в общем случае одинаковые в разных местах программы операции выполняются над разными аргументами. Выделение подпрограмм далее понимается как выделение упорядоченной совокупности повторяющихся в разных местах программы операций, перед которой могут стоять неповторяющиеся операции.

Установим произвольным образом однозначное соответствие между элементами O_ξ множества O и цифрами натурального ряда 1,2,…Z. Таким образом, каждая операция $O_\xi \in O$ окажется помеченной некоторой цифрой, операторы $a_i \in A$ также будут помечены цифрами, но при этом двум различным операторам a_i и a_j сожжет соответствовать одна цифра. Условимся, что $f(a_j) = f_j$ есть число, которым обозначен оператор a_j. Программа работы СЗИ и центрального компьютера теперь будет представлять последовательность цифр из диапазона $1 \div Z$, длина ее $x = M$.

Цель работы. Выделить из заданной программы L все возможные подпрограммы $L_i = B_i \in B$, где B - полное множество подпрограмм.

Основная часть. На основании поставленной цел найдем подмножество подпрограмм $\left\{\tilde{c}^i\right\} \subset \tilde{c}$, делающее оптимальное покрытие L. Для решения первой задачи составляется матрица $W^1 = \left\| w_{ij}^1 \right\|$, строки и столбцы которой соответствуют операторам $a_i \in A$, расположенным в порядке следования их в программе L, а

$$w_{ij}^1 = \begin{cases} w_{ij}\left(w_{i-1,j-1} \vee w_{i+1,j+1}\right), \text{åñëè \_}\, i \prec j; \\ 0, \text{åñëè \_}\, i \geq j, \end{cases} \tag{1}$$

где

$$w_{ij} = \begin{cases} 1, \text{åñëè \_}\, f\left(a_i\right) = f\left(a_j\right), \\ 0, \text{åñëè \_}\, f\left(a_i\right) \neq f\left(a_j\right). \end{cases} \tag{2}$$

Нетрудно видеть, то матрица W^1 задает некоторое отношение $E \subset L^1 \times L^2$, причем $L^1 = L^2 = L$, а индексы 1 и 2 поставлены для различия строк и столбцов матрицы W^1 в связи с несимметричностью отношения E. Обозначим последовательности единиц (каждая из которых соответствует некоторой подпрограмме), полученные в W^1 в результате применения (1) и (2), через $B_i \in B$, $i = 1 \div n_1$.

Таким образом, B представляет собой полное множество подпрограмм.

Проектируя $B_i \in B\left(i = 1 \div n_1\right)$ на L^1, получаем множество P упорядоченных подмножеств $B_i \in B\left(i = 1 \div n_1\right)$ операторов, причем $n_2 \leq n_1$, так как несколько B_i могут меть одну проекцию P_j. Учитывая, что в общем случае $P_i \cap P_j \neq \varnothing$, выделим все связные (по отношения к строке L) множества $C_j = \cup P, j = 1 \div n_3, n_3 \leq n_2$, каждое из которых разобьем на сумму непересекающихся подмножеств $C_j = \bigcup\limits_{i \in I^i} C_i^i, C^i \cap C^k = \varnothing, i \in I^i = 1 \div n_4, n_4 \geq n_3$ следующим образом.

Пусть $I_j = 1 \div k_1$, тогда $C_j = \bigcup\limits_{i=1}^{k_1} P_i = \bigcup\limits_{i=1}^{k_2} C^i$, где C^i при $i = 1 \div k_2$ определяется как

$$C^1 = \bigcap_{i=1}^{k_1} P_i;$$

$$C^2 = \bigcap_{i=1}^{k_1-1} P_i \setminus C^1;$$

$$C^3 = \bigcap_{i=1}^{k_1-2} P_i \cap P_{k_1} \setminus C^1; \ldots, C^{i_1} = \left(\bigcap_{i=1}^{k_1-i_1+1} P_i\right) \cap \left(\bigcap_{i=k_1-i_1+3}^{k_1} P_i\right) \setminus C^1; \ldots$$

$$C^{\left(k_2^1\right)+1} = \bigcap_{i=2}^{k_1} P_i \setminus C^1; \tag{3}$$

$$C^{\left(k_2^1\right)+2} = \bigcap_{i=1}^{k_1-2} P_i \setminus \bigcup_{i=1}^{\left(k_2^1\right)+1} C^i$$

и т.д.

Получим все $C^i \in C_j \subset C, j = 1 \div n_3, i = 1 \div n_4$. Для полученных C^i найдем $\mu\left(C^i\right) = \mu_i$, где μ_i - мера множества. Исключим из C все множества с $\mu_i \prec 2$; наполним его совокупностью множества P, а также совокупностью связных упорядоченных подмножеств из $L \setminus \bigcup\limits_{i=1}^{n_2} P_i$, после чего поучим систему (множество) $\tilde{C} = \left\{\tilde{C}^i\right\}, i = 1 \div n_6$, где $\tilde{C}^i$ есть C^i или P_i, или связное множество из $L \setminus \bigcup\limits_{i=1}^{n_2} P_i$.

Система множеств $\overset{\square}{E}$ порождает разбиение множества L^2 на ряд связных подмножеств $D_i \subset L^2$ следующим образом. Каждому $\overset{\square}{E}^i$ становится в соответствие совокупность упорядоченных подмножеств $D_i \subset L^2$, $\overset{\square}{E}^i \Rightarrow \{D_i\}$; причем каждое D_i состоит из элементов $a_i \in A$, образующих связное подмножество и являющихся сечениями элементов из $\overset{\square}{E}^i$ по отношению $R \subset L^1 \times L^2$; R получается из E добавлением диагонали. В общем случае $D_j \cap D_j \neq \varnothing$, причем $\underset{i}{\cup} D_i = L^2$. Используя (3), разобьем L^2 на систему подмножеств $D^i \in D, i = 1 \div n_7$, для которой $\underset{i}{\cup} D_i = L^2, D_i \cap D_i \neq \varnothing$, после чего каждому $\overset{\square}{E}^i$ окажется поставленным в соответствие подмножество $\overset{\square}{D}^i = \{D^j\} \subset D; \overset{\square}{E}^i \Rightarrow D^i = \{D^j\}$. Данное соответствие $\overset{\square}{E}^i \Rightarrow \{D^j\}$ задается отношением $S \subset \overset{\square}{E} \times D$, которое может быть представлено матрицей $K_0 = \left\| k_{ij}^0 \right\|$, причем $k_{ij}^0 = 1$, если $\overset{\square}{D}^j = \overset{\square}{D}^i$, что свидетельствует о том, что D^j может быть покрыто $\overset{\square}{E}^i$. Строкам и столбцам матрицы приписываются веса, равные $\mu\left(\overset{\square}{E}^i\right) = \overset{\square}{\mu}^i, i = 1 \div n_6, \mu\left(D^j\right) = \mu_j, j = 1 \div n_7$.

Для выбора квазиоптимальной системы покрытой $\left\{\overset{\square}{E}^i\right\} \subset \overset{\square}{E}$ предлагается следующий алгоритм.

Шаг 1. Для каждой строки матрицы K_0, задающей соответствие $\overset{\square}{E}^i \Rightarrow \overset{\square}{D}^i = \{D^j\}$, вычисляется:

$$a_i^0\left(\overset{\square}{E}^i\right) = \frac{\mu\left(\overset{\square}{E}^i\right) + \dfrac{\mu\left(\{D^j\}\right)}{\mu\left(\overset{\square}{E}^i\right)}}{\mu\left(\{D^j\}\right)} = \frac{\left(\mu\left(\overset{\square}{E}^i\right)\right)^2 + \mu\left(\{D^j\}\right)}{\mu\left(\overset{\square}{E}^i\right) \cdot \mu\left(\{D^j\}\right)} \quad (4)$$

Из самого принципа построения матрицы K_0 следует, что $\dfrac{\mu\left(\{D^j\}\right)}{\mu\left(\overset{\square}{E}^i\right)}$ есть целое число.

Учитывая, что $D^i \cap D^j \neq \varnothing$, имеем $\mu\left(\{D^j\}\right) = \sum\limits_{j\left(\overset{\square}{D}^i\right)} \mu\left(D^j\right)$, тогда

$$a_i^0\left(\overset{\square}{E}^i\right) = \frac{\left[\mu\left(\overset{\square}{E}^i\right)\right]^2 + \sum\limits_{j\left(\overset{\square}{D}^i\right)} \mu\left(D^j\right)}{\mu\left(\overset{\square}{E}^i\right) \cdot \sum\limits_{j\left(\overset{\square}{D}^i\right)} \mu\left(D^j\right)} \quad (5)$$

Шаг 2. Выбирается

$$a_w^0\left(\overset{\square}{E}^{w_0}\right) = \min_i \left\{a_i^0\left(\overset{\square}{E}^i\right)\right\} \quad (6)$$

Если $a_w^0\left(\overset{\square}{E}^{w_0}\right) \geq 1$, то выполняется шаг 3, в противном случае из матрицы K_0 строится новая матрица $K^1 = \left\| k_{ij}^1 \right\|$ с учетом следующего:

а) $\tilde{C}^{w_0} = P_j \notin P$. В этом случае матрица K^1 получается из матрицы K_0 вычеркиванием строки, соответствующей $\tilde{C}^{w_0}$ и столбцов D_j, для которых $\tilde{C}^{w_0} \Rightarrow \tilde{D}^{w_0} = \{D^j\}$;

б) $\tilde{C}^{w_0} \subset P_{j_1}, \tilde{C}^{w_0} \subset P_{j_2}, ..., \tilde{C}^{w_0} \subset P_{j_k}$, т.е. $\tilde{C}^{w_0} = C^i$ получено согласно (3).

Выделение $\tilde{C}^{w_0}$ разбивает связное подмножество P_{ji}, $i = 1 \div k$ на два связных подмножества:

$P_{ji}^{\delta} \subset P_{j1}; P_{ji}^{\delta} \cap P_{ji} = P_{ji}^{\delta}; P_{ji}^{1} \cap P_{ji}^{2} = \varnothing; \delta = 1,2; i = 1 \div k$, при этом $P_{ji}^{\delta} = \bigcup_{n_1, n_2, ... n_{d\delta}} C^n$; $C^{n_i} \cap C^{n_j} = \varnothing$.

В частном случае $P_{ji}^{1} = \varnothing; P_{ji}^{2} \neq \varnothing$ или $P_{ji}^{1} \neq \varnothing$; $P_{ji}^{2} = \varnothing$.

Матрица K^1 тогда получается:

1. Вычеркиванием строки, соответствующей $\tilde{C}^{w_0}$ и столбцов D^j, для которых $\tilde{C}^{w_0} \Rightarrow \tilde{D}^{w_0} = \{D^j\}$.

2. Вычеркиванием строк, соответствующих $P_{ji,i}; i = 1 \div k$.

3. Добавлением строк, соответствующих $\tilde{C}^{n_6+\Omega} = P_{ji}^{\delta} = \bigcup_{n_1, n_2, ... n_{d\delta}} C^n, i = 1 \div k, \delta = 1,2$ если $d_{\delta} \geq 2$. Соответствие $\tilde{C}^{n_6+\Omega} = P_{ji}^{\delta} \Rightarrow \tilde{D}^{n_6+\Omega} = \{D^j\}$ добавленных строк столбцами матрицы K^1 получается из $\tilde{C}^{a} = P_{ji} \Rightarrow \tilde{D}^{a} = \{D^j\}$ и $\tilde{C}^{w_0} \Rightarrow \tilde{D}^{w_0} = \{D^j\}$, при этом

$$\tilde{D}^{n_6+\Omega} = \tilde{D}^{a} \setminus \tilde{D}^{w_0}. \tag{7}$$

Веса новых строк вычисляются как

$$\mu\left(\tilde{C}^{n_6+\Omega}\right) = \mu\left(P_{ji}^{\delta}\right) = \tilde{\mu}_{n_6+\Omega} = \mu\left(\bigcup_{n_1, n_2, ... n_{d\delta}} C^n\right) = \sum_{n_1, n_2, ... n_{d\delta}} \mu\left(C^n\right). \tag{8}$$

После выполнения шага 2 производится к шагу 1,2; снова для каждой строки матрицы K^1 вычисляется $a_i^1\left(\tilde{C}^i\right)$ по формуле (5) и выбирается $a_w^1\left(\tilde{C}^{w_i}\right) = \min_i \left\{a_i^1\left(\tilde{C}^i\right)\right\}$ согласно (6), только теперь при нахождении $\mu\left(\{D^i\}\right) = \sum_{j(D^i)} \mu\left(D^i\right)$ в суммировании не участвуют столбцы, вычеркнутые на предыдущем шаге.

Таким образом, в ходе выполнения алгоритма производится последовательное построение матриц $K^0, K^1, K^2, ..., K^i$ и т.д. K^{β}, а также вычисление и нахождение $a_w^0\left(\tilde{C}^{w_0}\right), a_w^1\left(\tilde{C}^{w_1}\right), ..., a_w^{\beta}\left(\tilde{C}^{w_{\beta}}\right)$, соответствующих $\tilde{C}^{w_0}, \tilde{C}^{w_1}, ..., \tilde{C}^{w_{\beta}}$.

Шаг 3. Составляется квазиоптимальная система покрытий $\left\{\tilde{C}^i\right\} = \tilde{C}$, которая включает в себя :

1. Подпрограммы $\left\{\tilde{C}^{w_0}, \tilde{C}^{w_1}, ..., \tilde{C}^{w_{\beta}}\right\}$, соответствующие строкам, вычеркнутым при выполнении шагов 1 и 2. Их длина и количество повторений определятся соответственно как

$$x_{w_i} = \mu\left(\tilde{C}^{w_i}\right); y_{w_i} = \frac{\mu\left(\{D^j\}\right)}{\mu\left(\left\{\tilde{C}^{w_i}\right\}\right)}; i = 1 \div \beta, \tag{9}$$

при условии $\vec{C}^{w_i} \Rightarrow \vec{D}^{w_i} = \{D^j\}$.

2. Подпрограммы D^j, соответствующие столбцам, оставшимся не вычеркнутыми после выполнения шагов 1 и 2. Для них $x_j = \mu(D^j)$, а $y_j = 1$.

Выводы. Следует отметить, что при реализации программы L выделению из общей последовательности операторов подлежат лишь подпрограмм, удовлетворяющие шагу 3.1, так как только они дат выгоду в числе команд, равную

$$\Delta = \sum_{i=1}^{\beta}\left[x_{w_i} y_{w_i} - \left(x_{w_i} + y_{w_i}\right)\right] = \sum_{i=1}^{\beta}\Delta_i .$$

ЛИТЕРАТУРА:

1. Згуровский М.З. – Основи системного аналізу / Згуровський М.З., Понкратова Н.Д. – К.: Видавн. група BHV, 2007. – 544с.

2. Фельдман Л.П. – Чисельні методи в інформатиці / Фельдман Л.П., Петренко А.І., Дмитрієва О.А. – К.: Видавн. група BHV, 2006. – 480с.

Рецензент: д.т.н., проф. Лєнков С.В.