4.2. Размещение элементов защиты информации по критерию “эффективность-стоимость”

Представляется возможным исследование оценки эффективности и размещения элементов СИБ в автоматизированных информационных (государственных и коммерческих) системах. В качестве основных характеристик используем производительность и стоимость СИБ [110,167,60, 131]. При отсутствии механизмов защиты нарушителю не требуются серьезные усилия для получения доступа. В АИС со слабой защитой усилия нарушителя пропорциональны затратам на обеспечение безопасности. Системы с высоким уровнем защиты характеризуются тем, что незначительные усилия по обеспечению безопасности приводят к существенному повышению затрат нарушителя для получения несанкционированного доступа. В условиях создания идеальной системы защиты [132], что возможно только при больших затратах, нарушитель прилагает непомерно высокие усилия для преодоления механизмов СИБ.

Для решения данной проблемы необходимо использовать методы динамического программирования; смешанного целочисленного линейного программирования; эвристические методы [167].

При использовании динамического программирования АИС представляется в виде гибридной структуры, сочетающей древовидный и сетевой графы, соединенных ориентированными дугами. Решение проблемы размещения и оценки СИБ в узлах АИС формулируется следующим образом: целесообразно ли устанавливать соответствующий тип СИБ (или несколько типов одновременно) в каждом узле, и если целесообразно, то какой тип СИБ следует установить. Для математического описания могут быть использованы следующие данные:

d_i - запрос (сообщение), поступающий в узел сети;

p_1, p_2, p_{12} - стоимость установки СИБ первого типа, второго типа и обоих типов одновременно;

ρ_1, ρ_2 - коэффициенты стоимости передачи запроса (сообщения) для СИБ первого и второго типов ($\rho > 1$);

c_{ij} - стоимость передачи одного запроса (сообщения), необработанного в плане СИБ, по линии (i,j);

b_{ij} - стоимость передачи одного запроса (сообщения), обработанного в плане СИБ, по линии (i,j);

p_i - стоимость передачи одного блока обработанных данных из узла i в следующую точку;

q_1, q_2 - приращение стоимости для СИБ первого и второго типов;

R_i - множество узлов, непосредственно связанных с узлом i;

$s(i)$ - узел, следующий за узлом i;

$s_2(i) = s(s(i))$; $s_m(i)$ - узел, следующий за узлом через $(m-1)$ узел;

b_{ilm} - стоимость передачи блока данных, поступающих в узел i из узла $s(i)$;

Значения b вычисляются с использованием следующих рекурсивных соотношений:

для $j=s(i)$ и $k=s(i)$

$$b_{i11}=p_i$$

$$b_{ilm}=b_{jk}+b_{i\,l\,m-1} \qquad \text{для } m>2 \tag{4.13}$$

$$b_{ilm}=c_{ik}+b_{i\,l-1\,m-1} \qquad \text{для } m>l>2$$

и если N - выбранная точка сети и $i \in R_N$, то $b_{i11}=0$.

После этого имеется возможность определения лучшего варианта размещения СИБ (по критерию стоимости с условием обеспечения заданного уровня надежности) для поддерева с корнем в узле i :

$$min\{Z^0, Z^1, Z^2, Z^3\} \tag{4.14}$$

где Z - стоимость четырех вариантов СИБ для сети (Z^0 - СИБ отсутствует и заменена внешним организационно-техническим контуром, Z^1- только СИБ первого типа, Z^2 - СИБ второго типа, Z^3 - СИБ обоих типов).

Введем следующие дополнительные условные обозначения:

f_{ilm} - стоимость варианта для всего трафика, входящего в узел i, при условии, что первый тип СИБ, через который пройдет поток данных

после узла *i*, встретится в узле $s_l(i)$, а второй тип СИБ в узле $s_l(i)$ или $s_m(i)$ при условии, что $1 < l < m$;

g_{ilmv} - стоимость варианта для всего трафика, входящего в узел *i*, при условии, что первый тип СИБ, через который пройдет поток данных после узла *i*, встретится в узле $s_l(i)$, второй тип СИБ в узле $s_m(i)$, а следующий второй тип СИБ в узле $s_l(i)$ или $s_v(i)$ при условии, что $1<m<l<v$.

Тогда для $j=s(i)$ и $1 < m$, получаем:

$$f_{ilm} = \min\{Z^r_{ilm} | r = 0,1,2,3\};$$

$$Z^0_{ilm} = (c_{ij} + \beta_{ilm})d_i + \sum_{h \in R_i} f_{hl+1m+1}; \qquad (4.15)$$

$$Z^1_{ilm} = Z^1_i = p_1 + (b_{ij} + \beta_{ilm}) d_i \rho_1 + \sum_{h \hat{I} R_i} f_{hlm+1} \text{ для всех } l;$$

$$Z^2_{ilm} = Z^2_i = p_2 + (c_{ij} + \beta_{ilm}) d_i \rho_2 + \sum_{h \hat{I} R_i} f_{hl+1m+1};$$

$$Z^3_{ilm} = Z^3_i = p_{1,2} + p_i d_i \rho_1 \rho_2 + \sum_{h \hat{I} R_i} f_{hl+1}; \text{ для всех l и m;}$$

для $j=s(i)$ и $m < l < v$ получаем:

$$g_{ilmv} = \min\{Y^r_{ikmv} | r = 0,1,2,3\} \qquad (4.16)$$

где *Y* определяется аналогично *Z*.

При использовании смешанного целочисленного программирования отпадает необходимость в предварительном определении деревьев для каждого узла и считается, что данные могут передаваться в любом направлении. Для данного случая необходимо минимизировать стоимостную функцию, учитывающую размещение типов системы ИБ.

При использовании эвристических алгоритмов задача формулируется следующим образом: необходим выбор минимальной по стоимости СИБ, обеспечивающей прохождение от выбранной точки *i* сети к рассматриваемому узлу, при обеспечении требуемого уровня надежности. Для данного случая минимальное по стоимости решение ***d(z)*** из заданного множества типов СИБ может быть получено из следующего уравнения:

$$d_i(z)=\sum_{m=1}^{M} P_{m_{i=1}} * \sum_{i=1}^{N} z_{im} + \sum_{i=1}^{N} d(c) D_i \qquad (4.17)$$

где $d_i(c)$ - стоимость минимального трафика из узла i к следующей точке сети для множества типов системы ИБ.

Выбор конфигурации системы ИБ для АИС может быть осуществлен на основе итераций путем исключения конкретного типа СИБ без снижения общего уровня надежности. Для описания алгоритма выбора конфигурации введем следующие обозначения:

$z^t=\{p_{im}; z^t_{im}\}$ - множество типов СИБ для итерации t;

z^t_{im} - новое множество типов системы ИБ, полученное путем исключения конкретного типа СИБ p_{im} в узле i уровня m сети.

Итерационный процесс может быть описан следующим образом:

Шаг 0: t=0; z^0 - все типы СИБ находятся в каждом узле.

Шаг 1: Пробное исключение одного из типов СИБ из z^t .

Для каждого p_{im} такого, что z^t_{im}=1 вычисляется $c_l(z^t_{im})$ - общая минимальная стоимость трафика при наличии множества типов СИБ z^t_{im} .

Шаг 2: Для исключения типа СИБ определяется:

$$d(z^t_{i_t m_t})=\min p_{im} d(z^t_{im}) \qquad (4.18)$$

Если $d(c^t_{i_t m_t})>d(z^t_{im})$, то алгоритм прекращает работу, поскольку дальнейшее уменьшение стоимости (при сохранении требуемого уровня надежности) невозможно. В противном случае тип системы ИБ исключается:

$$z^{t+1}=z^t_{i_t m_t} \qquad (4.19)$$

$d(z^{t+1})=d(z^t_{i_t m_t})$ при $t=t+1$

Переход к шагу 1.

Решение данной задачи может быть выполнено также с помощью гибридного метода, объединяющего имитационные и аналитические модели. К преимуществам такого подхода относятся следующие: существенное уменьшение сложности модели; возможность обнаружения

критических элементов; повышение чувствительности модели к внешним и внутренним возмущениям; простота реализации и др.

Введем следующие дополнительные условные обозначения. Пусть АИС состоит из M компонентов (N - узлов и L коммуникационных линий, причем $M=N+L$). Стохастический процесс $X(t)=(X_1(t),...,X_M(t))$ определяет функциональный статус сетевых компонент следующим образом:

$$X_k(t) = \begin{cases} 1, \text{ если компонента находится в работоспособном состоянии в момент времени } t; \\ 0, \text{ в противном случае, для } k=1,...,M. \end{cases}$$

Область состояний АИС Ω_x содержит 2^M различных состояний. Пусть $p(x)$ определяет вероятность устойчивого состояния для тех случаев, когда глобальное состояние АИС равно x. Для глобального состояния x параметра АИС описываются следующим образом:

$$Y(x)=(Y_1(x),...,Y_M(x)), \qquad (4.20)$$

область состояний которого равна Ω_y.

Для характеристики устойчивого состояния АИС с точки зрения СИБ может использоваться достаточное количество показателей, в их числе такие, как средняя задержка данных, среднее время вызова узла, вероятность блокировки и многие др. Процесс считается устойчивым, если при возникновении отказа или изменении глобального состояния, поток данных в АИС переходит в состояние равновесия. Это означает, что при изменении состояния АИС (например, из x в x') устойчивое состояние $Y(x)$ переходит в устойчивое состояние $Y(x')$ без отклонения. В свою очередь, область Ω_y, может быть разделена на два следующих подмножества:

- подмножество S, характеризующее допустимое состояние АИС с сохранением функциональных характеристик;

- подмножество $F\ (\Omega_y - S)$, характеризующее состояние АИС с характеристиками ниже допустимого.

Как отмечалось выше, для характеристики состояния АИС может использоваться множество показателей. Их можно представить в виде вектора показателей эффективности. Один из возможных вероятностных показателей может быть описан следующим образом:

$$\sum_{x\hat{I}\,\Omega_x} P\{Y(x)\,\hat{I}S\} * p(x) \quad . \qquad (4.21)$$

В свою очередь, средняя характеристика *i*-го компонента вектора показателей эффективности *Y(x)* рассчитывается следующим образом:

$$\sum_{x\hat{I}\,\Omega_x} E[Y_i(x)] * p(x) \qquad i=1,\ldots,n.$$

(4.22)

Множество состояний, характеризующих множества Ω_x и Ω_y, могут включать достаточно большое их количество, что делает практически невозможным расчет полной суммы. Для исключения подобного необходимо ограничить расчет суммы только в выбранных точках (например, в точке *x*), которая выбирается на основе следующего условия:

$$p(x) > \beta \ , \qquad (4.23)$$

где β - бесконечно малое число.

В свою очередь, среднюю характеристику *i*-го компонента вектора показателей эффективности можно представить следующим образом:

$$\sum_{x\hat{I}\,\Omega_{(\beta)}} E[Y_i(x)] * p(x) \ ,$$

(4.24)

где $\Omega(\beta) = \{x : p(x) > \beta\}$ . .

Применительно к данному выражению представляется возможным объединение имитационного моделирования по методу Монте-Карло с аналитической моделью в следующей последовательности итерационных операций.

Шаг 1. С помощью имитационной модели получают состояние x_i из множества Ω_x в соответствии с распределением вероятности *p(x)*.

Шаг 2. На основе рассчитанного, с использованием аналитических зависимостей состояния x_i определяются следующие показатели:

$P\{Y(x_i)\hat{I}S\}$

$E[Y_j(x_i)]$ для $j=1,...,m.$ (4.25)

Шаг 3. После n повторов вычислений приведенных показателей оценивается общий коэффициент готовности по следующей формуле:

$$n^{-1}*\sum_i P\{Y(x_i)\hat{I}S\}, \quad (4.26)$$

и значение среднего j-го компонента показателя эффективности

$$n^{-1}*\sum_i E[Y_j(x_i)] \quad \text{для } j=1,...,m. \quad (4.27)$$

Функция вероятности $p(x)$ рассчитывается по следующей формуле:

$$p(x)=\prod_{k=1}^{M} p_k^{x_k}(1-p_k)^{1-x_k}, \quad (4.28)$$

где $p_k=p$ {компонент k исправен и обеспечивает требуемый уровень надежности} при $k=1,...,M$. Для тех случаев, когда отмечаются зависимые друг от друга отказы и сбои, вызванные неисправностями и срывами компонент системы ИБ, состояние сети генерируется с помощью следующих итераций.

Шаг 1. Определяется вектор $x=(x_1,...,x_M)$ с использованием распределения, приведенного в (3.66).

Шаг 2. Если $s(k)$ определяет множество соседних с k-м компонентом системы ИБ и на первом этапе $x=0$, то для всех $j\hat{I}S(k)$ рассчитывается состояние в соответствии со следующим распределением:

$$p\{x_j=1\} = 1 - p\{x_j = p_{j/2}\} \quad (4.29)$$

Другими словами, на первом этапе генерируются возможные отказы компонент системы ИБ сети с вероятностью $p(x)$. На втором этапе генерируются отказы только тех узлов, которые соединены с отказавшими компонентами СИБ на первом этапе.

Для оценки функционирования АИС с точки зрения безопасности можно использовать также показатель $C_g=p$ (все узлы сети доступны), то есть

$$Y_j(x)= \begin{cases} 1, \text{ если все узлы доступны;} \\ 0, \text{ в противном случае.} \end{cases}$$

Возможно использование и другого показателя - вероятности того, что узел *j* доступен всем узлам, включенным в множество s*(i)*, то есть

$$C_{j,s(j)}(x)=\begin{cases}1, \text{ если узел } j \text{ доступен всем узлам } i\hat{I}s(j);\\ 0, \text{ в противном случае.}\end{cases}$$

С целью оптимизации характеристик АИС можно получить также информацию о чувствительности системы к изменению СИБ, используя метод малого периметра. С этой целью запишем общий показатель эффективности сети в виде следующего выражения:

$$MP=\sum_x P\{Y(x)\hat{I}S\}p(x). \qquad (4.30)$$

Соответственно компоненты будут определены как

$$MP=\sum_x E[Y_i(x)]p(x), \quad i=1,...,m. \qquad (4.31)$$

В данном случае функция вероятности может зависеть от значения вектора параметров $Q=(Q_1,Q_2,\ldots,Q_i)$, где $Q\hat{I}\,Q$ (через Q обозначим множество допустимых значений Q). Тогда (3.68 и 3.69) примут следующий вид:

$$MP(Q)=\sum_x P\{Y(x)\hat{I}S\}p(x;Q), \qquad (4.32)$$

$$MP(Q)=\sum_x E[Y_i(x)]p(x;Q), \quad i=1,...,m. \qquad (4.33)$$

Следующей задачей является оптимизация размещения элементов СИБ по критерию ценности информации, содержащейся в конкретном узле АИС, а также уязвимости соответствующего узла по отношению к группам программных злоупотреблений. Рассмотрим практическую реализацию рассмотренных задач. На рис.15 приведена топология гипотетической АИС, на основе которой построена матрица взаимосвязей СИБ (таб. 4). Реализация рассматриваемых моделей оценки эффективности и размещения элементов СИБ позволяет получить схему размещения (табл. 5.) с условием сохранения необходимого уровня надежности.

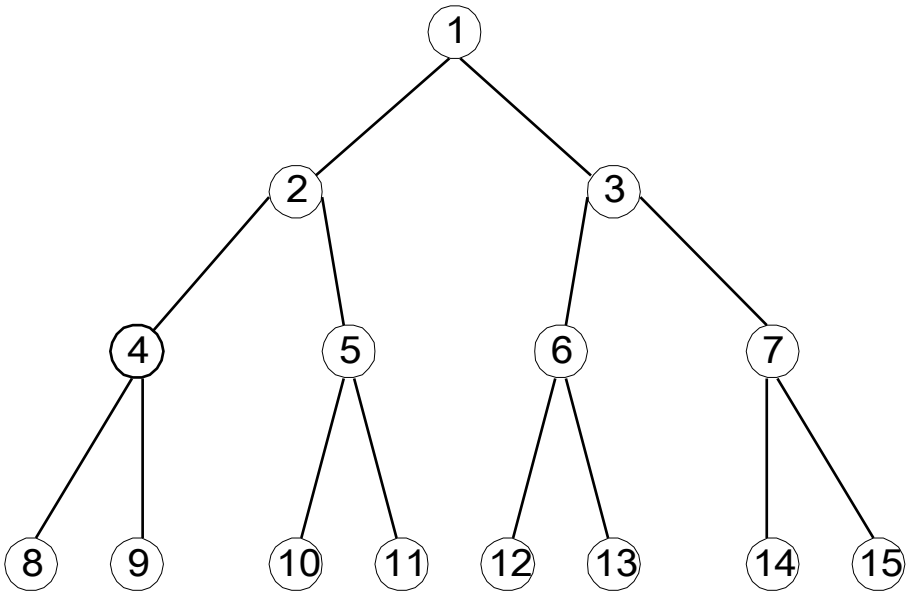

Рис. 15 *Архитектура гипотетической АИС*

Таблица 4

Матрица взаимосвязей узлов гипотетической АИС

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0
3	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0
4	0	1	0	1	0	0	0	1	1	0	0	0	0	0	0
5	0	1	0	0	1	0	0	0	0	1	1	0	0	0	0
6	0	0	1	0	0	1	0	0	0	0	0	1	1	0	0
7	0	0	1	0	0	0	1	0	0	0	0	0	0	1	1
8	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0
9	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0
10	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
11	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
12	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0
13	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
14	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
15	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

Таблица 5

Размещение СИБ в узлах гипотетической АИС

Узел	Тип СИБ
1	2

2	1
3	1
4	0
5	0
6	0
7	0
8	3
9	3
10	3
11	3
12	3
13	3
14	3
15	3

Необходимо решение дополнительной задачи размещения элементов СИБ по критерию стоимости. В качестве целевой функции задается стоимость СИБ и с помощью последовательных итерационных операций расчета показателей эффективности определяют максимальный уровень надежности с учетом степени риска нарушения целостности.

Приведенный комплекс алгоритмов может служить основой для оценки эффективности и размещения системы информационной безопасности.

Описаный подход позволяет разместить СИБ с условием сохранения необходимого уровня надежности. Но может возникнуть ситуация, когда в сети размещается СИБ с заданными показателями стоимости. Для решения подобной задачи задают функцию стоимости, и методом перестановок и пересчета показателей эффективности получают максимальный уровень надежности от размещения СИБ в сети при заданном уровне затрат.

Следующей, требущего решения задачи является анализ размещения элементов СИБ в узлах АИС.

Формулировка задачи: какова наибольшая вероятность того, что нарушитель проникнет в АИС через узел *i* и из него кратчайшим путем попадет в узел *j*.

Решение задачи необходимо в тех случаях, когда определенный узел является критическим (то есть содержит критичную для АИС информацию) и необходим анализ риска по отношению к данному конкретному узлу.

В качестве конечной цели решения данной задачи - определение количественной величины, отражающей максимальный уровень риска при определенной конфигурации средств обеспечения безопасности информации.

Для решения модели введем следующие дополнительные обозначения:

n - количество узлов АИС;

P^o_i- вероятность нарушения работы СИБ в узле *i* , где *i=1..n*;

$P^o_i=(1-P_i)$, где P_i - вероятность правильной обработки злоупотребления системой информационной безопасности;

S(n,n) - матрица путей сообщения АИС;

C(n,n) - матрица первичных оценок.

Решение задачи включает реализацию следующих шагов:

Шаг 1. Формируется первоначальная матрица:

$$C_{ij} = \begin{cases} P^o_i & \text{,если } i=j; \\ 0 & \text{,если нет дуги;} \\ P^o_i * P^o_j & \text{,если } i \neq j. \end{cases} \quad \text{где } i=1..n,\ j=1..n \qquad (4.44)$$

Шаг 2. Положим *k=1*.

Шаг 3. Для всех *i*, $j \neq k$ вычисляем значения $c_{ij}=\max\{c_{ij}, c_{ik} * c_{kj}\}$.

Шаг 4. *k=k+1*.

Шаг 5. Если $k \leq n$, то переход к п. 3, в противном случае - к п. 6.

Шаг 6. Элементы полученной матрицы определяют наибольшую вероятность поражения узла *j*, при условии, что нарушитель входит в систему через узел *i*.

Построенный аппарат позволяет моделировать реальные ситуации и получить рекомендации по размещению элементов информационной безопасности АИС, а также анализировать полученные решения и результаты.