УДК 004.056.5:518:512.624.3 Бобок И.И., Кобозева А.А., Хорошко В.А.

КОЛИЧЕСТВЕННАЯ ОЦЕНКА ЗНАЧИМОСТИ ПРОИЗВОЛЬНОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ФУНКЦИОНИРОВАНИЯ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ СИСТЕМЫ

1. Введение

С конца прошлого века в теории управления начал развиваться «неклассический» подход к моделированию автоматизированных систем управления, основывающийся на аналогиях архитектуры и целей функционирования сложных технических и биологических систем [1-4], который до настоящего момента был ориентирован на нейросетевую элементную базу. Использование нейронных сетей не обеспечивает всех выдвигаемых к моделям требований, обладающих в итоге рядом существенных недостатков [5,6]. В [7] была предпринята попытка создания принципиально новой универсальной графово-матричной модели информационно-технологической системы (ИТС), основывающейся на принципах функционирования нервной системы человека (НСЧ). Основными математическими инструментами являлись теория возмущений, теория графов, матричный анализ.

Предложенная в [7] модель представляет из себя иерархическую схему - взвешенный граф со структурным соотношением «состоять из» (рис.1). Такая структура модели была выбрана не случайно. Иерархия – наиболее общий метод классификации, используемый человеком. Такая классификация воспроизводит первичную форму координации или организации: 1) корковых процессов, 2) их психических соотносительных понятий и 3) их выражения в символах и языках [8]. Кроме того, иерархические модели обладают рядом значимых преимуществ перед моделями других видов [9]:

1) дают возможность исследования «степени влияния» приоритетов на верхних уровнях на приоритеты элементов нижних уровней [9];
2) предоставляют подробную информацию о структуре системы;
3) являются, как правило, устойчивыми (малые возмущения вызывают малый эффект);
4) гибкими (добавления к хорошо структурированной иерархии не разрушают ее характеристик).

При предложенном подходе к решению задачи о моделировании ИТС важную роль играют весовые коэффициенты вершин (узлов) графа-модели, отвечающих элементам системы. Значения весовых коэффициентов должны быть такими, чтобы численно отражать реальную значимость любого средства защиты (или группы средств) для функционирования ИТС в целом, несмотря на их различие (технические, законодательные, программные и т.д. средства). Для обеспечения одного из основных принципов функционирования НСЧ, максимальной начальной приспособленности, весовые коэффициенты должны быть получены, исходя из практического опыта при максимальном использовании априорной информации [7].

До настоящего момента вопросы количественной оценки защищенности объектов, эффективности средств защиты информации, значимости этих средств для функционирования совокупной ИТС, возможностей противника, а также методики для таких оценок проработаны недостаточно. Для определения весовых коэффициентов узлов, отвечающих техническим средствам защиты, возможно использование метода, предложенного в [10,11]. Задача определения конкретных числовых значений остальных весовых коэффициентов до настоящего момента оставалась нерешенной.

Целью настоящей работы является разработка методики численной оценки реальной значимости произвольных средств защиты информации для функционирования ИТС, т.е. расчета приоритетов средств защиты по отношению к совокупной системе,

предусматривающей возможность определенного изменения этих приоритетов как способа моделирования результата атаки, предпринимаемой на ИТС, и ответа системы на эту атаку.

2. Понятие иерархии

Предложенная в [7] математическая модель ИТС, как уже было отмечено выше, представляет из себя иерархическую структуру. Определим строго понятие иерархии.

Пусть "≤"- бинарное отношение нестрогого порядка на некотором множестве X [12]. Для любого отношения $x \le y,\ x, y \in X$, можно определить отношение $x < y$, что означает $x \le y, x \ne y$. Говорят, что y покрывает x, если $x < y$ и не существует такого $t \in X$, что $x < t < y$.

Определение. Пусть X - конечное частично упорядоченное множество [12] с наибольшим элементом $\bar{x}$. Множество X есть *иерархия*, если существует такое разбиение X на подмножества L_k, $k = \overline{1,h}$, где $L_1 = \{\bar{x}\}$, что выполняются следующие условия:

1) $x \in L_k \Rightarrow x^- \subset L_{k+1},\ k = \overline{1,h-1}$, где $x^- = \{y \mid x \text{ покрывает } y\}$;

2) $x \in L_k \Rightarrow x^+ \subset L_{k-1},\ k = \overline{2,h}$, где $x^+ = \{y \mid y \text{ покрывает } x\}$.

Для каждого $x \in X$ существует весовая функция, сущность которой зависит от явления, для которого строится иерархия:

$$w_x : x^- \to [0,1], \quad \sum_{y \in x^-} w_x(y) = 1.$$

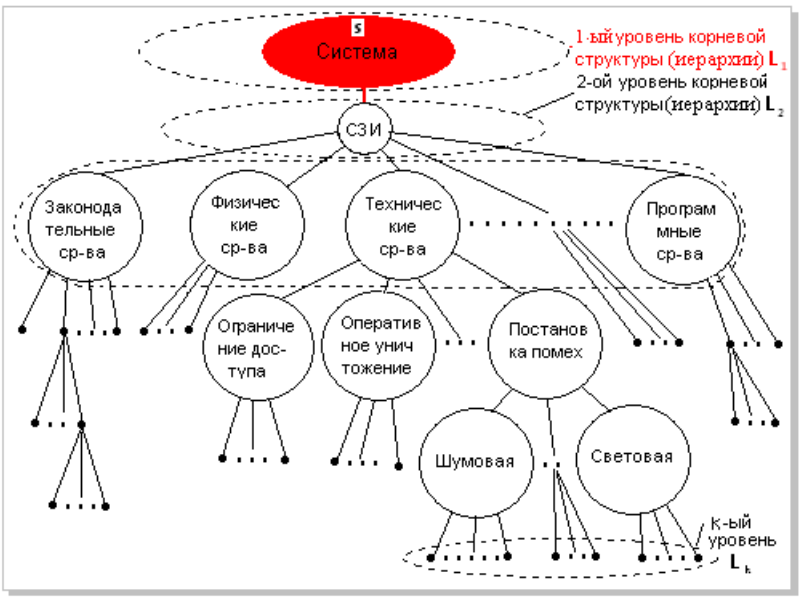

Рисунок 1. Структура уровней графовой модели ИТС.

Множества L_k называются уровнями иерархии, w_x - функция приоритета относительно элемента x.

Другими словами, иерархия есть определенный тип системы, основанный на предположении, что элементы системы могут группироваться в некоторые множества. Элементы каждой группы находятся под влиянием элементов некоторой вполне определенной группы и, в свою очередь, оказывают влияние на элементы другой группы. Будем считать, что элементы в каждой группе (уровне) иерархии независимы.

Очевидно, что предложенная в [7] модель ИТС (Системы) представляет из себя иерархию, для которой $L_1 = \{s\}$, где s отвечает совокупной Системе, а каждый уровень иерархии L_k является одновременно и уровнем корневой структуры графа-модели (рис.1).

Для достижения цели работы определим приоритеты элементов каждого уровня иерархии L_k по отношению к s, т.е. численно выразим значимость любого средства защиты (или совокупности средств) для функционирования Системы в целом, используя для этого метод анализа иерархий (МАИ) [9] с учетом особенностей построенной

иерархической модели. Такое выражение даст нам непосредственные значения весовых коэффициентов узлов графа Системы.

3. Методика определения весовых коэффициентов узлов графа-модели Системы

3.1. Сбор статистических данных

Первый шаг предлагаемой методики будет заключаться в накоплении статистических данных о работе ИТС .

Пусть анализ Системы проводится в течение времени T. Предполагается, что набор элементов, входящих в Систему, за время T не меняется. Пусть x_j отвечает конкретному средству защиты, которому в графовой модели соответствует вершина-лист (самый высокий уровень детализации). Среди имеющихся в распоряжении Системы средств защиты есть как постоянно действующие, так и включаемые при обнаружении попытки нападения [15]. Назовем *положительным исходом работы* x_j ситуацию, когда активация данного средства (в случае, когда x_j принадлежит ко второй группе) или его непрерывная работа (когда x_j принадлежит к первой группе) приводит к предотвращению несанкционированного доступа. Количество всех положительных исходов работы x_j за время T обозначим $k(x_j)$. Назовем *коэффициентом эффективной работы* $f(x_j)$ средства x_j отношение

$$f(x_j) = \frac{k(x_j)}{K},$$

где K - общее количество предпринимаемых попыток несанкционированного доступа к Системе за время T.

Накопление статистических данных происходит не только для отдельных средств защиты, но и для их совокупностей, в которые эти средства логически объединены при построении графа (вершины графа, не являющиеся листьями). Пусть несанкционированный доступ был предотвращен, например, при участии шумовой помехи. При сборе статистических данных такой случай приведет к увеличению на единицу количества положительных исходов работы непосредственно средства «шумовая помеха», совокупностей «постановка помех», «технические средства защиты» и т.д. (см.рис.1). Коэффициенты эффективной работы для совокупностей средств защиты будут определяться аналогично тому, как это было предложено выше для x_j. Заметим, что если $y_j \in L_k$ отражает некоторую совокупность средств, представленных на следующем уровне иерархии (корневой структуры) L_{k+1}, обозначаемых как $x_1, x_2, ..., x_n$, то в общем случае

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

где $k(y_j)$ и $f(y_j)$ - соответственно количество положительных исходов работы и коэффициент эффективной работы для совокупности y_j. Знаки неравенств в соотношениях (1) объясняются тем, что при построении математической модели невозможно учесть абсолютно все факторы, влияющие на функционирование совокупной Системы. Возможно, что в реальной Системе в состав y_j входит, кроме средств $x_1, x_2, ..., x_n$, еще $x_0, x_{-1}, ..., x_{-p}$, значимость которых настолько мала, что при построении модели они не были учтены отдельно.

Замечание 1. Сбор статистических данных необязательно проводить по анализу реальных атак на Систему. При моделировании любой ИТС необходимо, чтобы она оказалась адекватной предполагаемому противнику [15]. В силу этого будем считать, что нам известен набор $\{V_1, V_2, ..., V_l\}$ возможных атак. Моделируя физически эти атаки, частично или полностью искусственно «выводя из строя» то средство защиты, на которое направлена атака, проведем сбор необходимых данных, описанных выше.

Такой способ определения статистик дает возможность расширить набор имеющихся характеристик работы Системы, которые будут использованы ниже. Пусть атака V_j направлена непосредственно на средство x_i. Приведем искусственно Систему в состояние, соответствующее результату атаки V_j . Эту модифицированную Систему вместо исходной используем для накопления количества положительных исходов работы ее элементов, как было предложено выше. Проделаем это для каждой возможной атаки V_j. Пусть $x_1, x_2, ..., x_p$ - все множество средств защиты рассматриваемой Системы (множество листьев в графе-модели). Составим матрицу S:

	x_1	x_2	• • •	x_p
V_1	$k_{V_1}(x_1)$	$k_{V_1}(x_2)$	• • •	$k_{V_1}(x_p)$
V_2	$k_{V_2}(x_1)$	$k_{V_2}(x_2)$	• • •	$k_{V_2}(x_p)$
•	•	•		•
•	•	•		•
•	•	•		•
V_l	$k_{V_l}(x_1)$	$k_{V_l}(x_2)$	• • •	$k_{V_l}(x_p)$

где $k_{V_j}(x_m)$ - количество положительных исходов работы средства x_m в Системе, которая претерпела предварительно «безответную» атаку V_j. Если атака V_j полностью разрушила средство x_i, на которое была направлена, то $k_{V_j}(x_i) = 0$. По матрице S очевидно определяется матрица коэффициентов эффективной работы для описанных случаев модификации Системы.

Замечание 2. Использование коэффициентов эффективной работы в качестве весовых для соответствующих вершин графа-модели, которое, на первый взгляд, кажется возможным, нежелательно. Специфика предложенной в [7] модели Системы такова, что числовые значения весовых коэффициентов должны как можно точнее соответствовать реальной значимости каждого средства или совокупности средств для функционирования Системы, а статистические оценки достаточно точны лишь на очень больших выборках, что тяжело обеспечить. Однако общая тенденция *сравнительной значимости* разных средств защиты по отношению друг к другу для предотвращения несанкционированного доступа, т.е. для функционирования совокупной Системы, являющейся основной для получения весовых коэффициентов при выбранном способе построения модели, проявится быстрее.

В связи с замечанием 2 предпринимается следующий шаг в процессе построения весовых коэффициентов.

3.2. Определение первоначальных приоритетов элементов Системы

Второй шаг. Для оценки воздействия различных компонент на всю Систему и нахождения приоритетов этих компонент воспользуемся МАИ. Заметим, что иерархия графовой модели ИТС не является полной (иерархия называется полной, если для $\forall x \in L_k$ множество $x^+ = L_{k-1}$ при любом k). Более того, любая $x \in L_k$ смежна лишь с одной

вершиной, лежащей в предыдущем L_{k-1} уровне. Как будет показано ниже, эта особенность значительно снизит общий объем арифметических операций, необходимых для получения искомых значений приоритетов, по сравнению с количеством операций для общего случая полной иерархии.

Замечание 3. Независимо от того, будет ли иерархия полной, или для некоторого уровня L_k будет выполняться $x^- \neq L_{k+1}$, функцию w_x, фигурирующую в определении иерархии, можно единообразно определить для всех L_k, приравнивая ее к нулю для тех элементов в L_{k+1}, которые не принадлежат x^-.

Очевидно, количество уровней иерархии графа-модели больше двух. Пусть $x_1, x_2, ..., x_n$ - элементы одного уровня иерархии (вершины одного уровня корневой структуры графа Системы). Первоначально веса вершин $w_1, w_2, ..., w_n$ определяются весом влияния (приоритетом) $x_1, x_2, ..., x_n$ на смежный с ними элемент y_m предыдущего уровня. Для этого формируется матрица A размерности $n \times n$ парных сравнений силы влияния $x_1, x_2, ..., x_n$ на y_m, для чего используются полученные на первом шаге коэффициенты эффективной работы. Элементы a_{ij} матрицы A будем определять по следующему правилу [9]:

$$a_{ij} = \begin{cases} 1, \ \textit{если } f(x_i) \textit{ и } f(x_j) \textit{ имеют одинаковые значения} \\ 3, \textit{если } f(x_i) \textit{ незначительно больше } f(x_j) \\ 5, \textit{если } f(x_i) \textit{ значительно больше } f(x_j) \\ 7, \textit{если } f(x_i) \textit{ явно больше } f(x_j) \\ 9, \ \textit{если } f(x_i) \textit{ абсолютно превосходит } f(x_j) \end{cases}, \quad i, j = \overline{1,n},$$

хотя использование шкалы с целыми значениями $\{1,2,\ldots,9\}$, вообще говоря, не обязательно. Очевидно, $a_{ii} = 1, i = \overline{1,n}$, а для внедиагональных элементов: $a_{ij} = \frac{1}{a_{ji}}, \ i, j = \overline{1,n}$. Такая матрица A называется обратно-симметричной (reciprocal matrix [9]). Числа 2,4,6,8 и их обратные значения также могут использоваться при составлении матрицы попарных сравнений для облегчения компромиссов между немного отличающимися от основных суждениями.

Полученная матрица должна быть как можно более согласованной. В общем случае под согласованностью суждений подразумевается то, что при наличии основного массива необработанных данных все другие данные логически могут быть получены из них, используя отношение транзитивности [9]. Матрицу A назовем *согласованной*, если $a_{ik} = a_{ij} a_{jk}, \ \ i, j, k = \overline{1,n}$. Мерой согласованности выступает максимальное собственное (СЗ) матрицы A, а соответствующий собственный вектор (СВ) [13] обеспечивает упорядочение приоритетов. Действительно, очевидным для согласованности матрицы является случай, когда сравнения основаны на точных измерениях, т.е. $w_1, w_2, ..., w_n$ известны. Тогда

$$a_{ij} = \frac{w_i}{w_j}, \ \ i, j = \overline{1,n}, \tag{2}$$

$$a_{ij} a_{jk} = \frac{w_i}{w_j} \frac{w_j}{w_k} = \frac{w_i}{w_k} = a_{ik}, \quad i, j, k = \overline{1,n}.$$

Из (2) вытекает, что $a_{ij}\frac{w_j}{w_i}=1,\ i,j=\overline{1,n}$. Тогда $\sum_{j=1}^{n} a_{ij}\frac{w_j}{w_i}=n,\ i=\overline{1,n}$, или $\sum_{j=1}^{n} a_{ij}w_j=nw_i,\ i=\overline{1,n}$, а в матричном виде :

$$Aw=nw, \tag{3}$$

т.е. w - СВ A, соответствующий СЗ n.

Рассмотрим соотношение (3) подробнее. Поскольку элементы матрицы A определяются в соответствии с соотношением (2), то очевидно, что ее ранг равен единице, а ее спектр содержит единственное ненулевое собственное значение. Сумма СЗ матрицы и ее след $tr(A)$, где $tr(A)=\sum_{i=1}^{n} a_{ii}$, связаны соотношением [13]:

$$\sum_{i=1}^{n} \lambda_i = tr(A). \tag{3}$$

В силу свойств A, указанных выше, из (3) получаем, что

$$\sum_{i=1}^{n} \lambda_i = n, \tag{4}$$

тогда единственное ненулевое СЗ A, исходя из (4), определяется как $\lambda_{\max}=n$. В соответствии с теоремой Перрона [13], собственному значению $\lambda_{\max}$ соответствует СВ $w_{\max}$ матрицы A с положительными координатами. Для обеспечения единственности $w_{\max}$ будем рассматривать нормированные СВ. При этом норму вектора w определим как: $\|w\|=\sum_{i=1}^{n}|w_i|$. Тогда для $w_{\max}$ получим: $\|w_{\max}\|=\sum_{i=1}^{n} w_{\max i}=1$.

Таким образом, в случае согласованности матрицы A (идеальный случай) ее наибольшее СЗ равно n, более того, можно показать [13], что положительная обратносимметричная матрица согласована тогда и только тогда, когда $\lambda_{\max}=n$.

Однако выполнение требования (2) на практике нереально: никакие измерения не могут быть математически абсолютно точными, a_{ij} будут отклоняться от «идеальных» отношений $\frac{w_i}{w_j}$, а потому соотношение (3) не будет иметь места. Однако, принимая во внимание тот факт, что малые возмущения элементов a_{ij} положительной обратно-симметричной матрицы приведут к малым же возмущениям ее СЗ [9], можно слелать вывод, что $\lambda_{\max}$, являющееся максимальным СЗ при решении задачи

$$Aw=\lambda_{\max}w \tag{5}$$

с реально сформированной матрицей парных сравнений (элементы a_{ij} отклоняются от отношений $\frac{w_i}{w_j}$), останется близким к n, а остальные СЗ к нулю. Отклонение $\lambda_{\max}$ от n является мерой согласованности матрицы A, а отношение

$$(\lambda_{\max} - n)/(n-1) \qquad (6)$$

называется *индексом согласованности*. Удовлетворительным считается случай, когда значение (6) меньше или равно 0.1. Если получен индекс согласованности, превышающий 0.1, то допускается «пересмотр суждений», т.е. корректировка матрицы A. Одним из наиболее часто используемых для этого способов является итерационный метод последовательной корректировки на каждой итерации тех элементов A, для которых абсолютная разность между a_{ij} и $\frac{w_i}{w_j}$ является наибольшей, при помощи замены a_{ij} на $\frac{w_i}{w_j}$ и пересчета вектора приоритетов [9].

Установим теперь приоритет каждого элемента построенной иерархической модели ИТС относительно главной цели – Системы в целом. Иными словами, определим приоритеты (весовые коэффициенты) для вершин любого уровня корневой структуры графа-модели относительно вершины $s = L_1$, являющейся максимальным элементом иерархии (корнем дерева).

3.3. Определение окончательных приоритетов элементов Системы

Третий шаг. Пусть $Y = \{y_1, ..., y_{m_k}\} \subseteq L_k$, а $X = \{x_1, ..., x_{m_{k+1}}\} \subseteq L_{k+1}$. В соответствии с замечанием 2, можно предположить, что $Y = L_k$, $X = L_{k+1}$. Пусть элемент $z \in L_{k-1}$, такой, что любой элемент множества Y принадлежит множеству z^-. Для каждого элемента $x_i, i = \overline{1, m_{k+1}}$ определен приоритет этого элемента $w_{y_j}(x_i)$ по отношению к каждому элементу y_j, $j = \overline{1, m_k}$ предыдущего уровня. Для каждого элемента y_j из уровня иерархии L_k определен его приоритет $w_z(y_j)$ относительно $z \in L_{k-1}$ (рис. 2). Если через w обозначить функцию приоритета элементов из X относительно z, то

$$w(x_i) = \sum_{j=1}^{m_k} w_{y_j}(x_i) w_z(y_j), i = \overline{1, m_{k+1}}. \qquad (7)$$

Соотношение (7), по сути, представляет из себя процесс взвешивания приоритетов x_i относительно элементов y_j при помощи приоритетов y_j относительно z. Соотношение (7) может быть записано в матричном виде:

$$W = B\overline{W}, \qquad (8)$$

где элементы матрицы B определяются как $b_{ij} = w_{y_j}(x_i)$, $i = \overline{1, m_{k+1}}$, $j = \overline{1, m_k}$, элементы векторов $W, \overline{W}$ - это $w(x_i)$, $i = \overline{1, m_{k+1}}$, и $w_z(y_j)$, $j = \overline{1, m_k}$, соответственно. Таким образом, каждый процесс

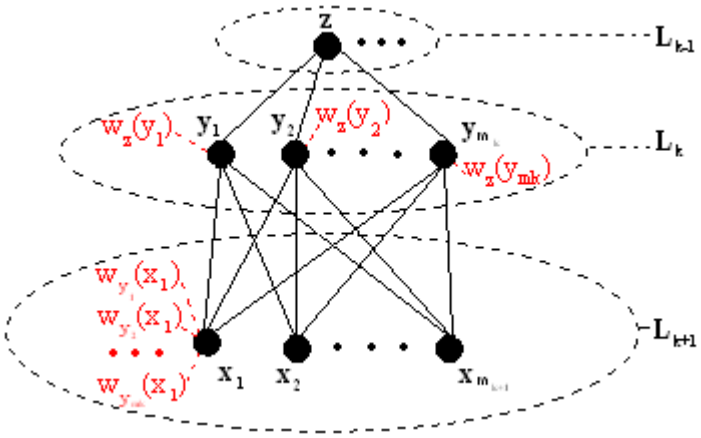

Рисунок 2. Последовательное определение приоритетов элементов иерархии

пересчета приоритетов элементов $x_1,..., x_{m_{k+1}}$ в соответствии с (8) потребует

$$O(m_{k+1}m_k) \qquad (9)$$

арифметических операций

Очевидно, процесс последовательного вычисления приоритетов $x_1,..., x_{m_{k+1}} \in L_{k+1}$ можно продолжить по индукции относительно элементов уровней $L_{k-2},..., L_1$, тем самым определяя приоритеты любого элемента иерархии относительно главной цели L_1.

Для неполной иерархии рассматриваемой графовой модели Системы пересчет приоритетов по формуле (7) потребует гораздо меньше вычислительных затрат, чем определено в соотношении (9). Каждый элемент $x_1,..., x_{m_{k+1}} \in L_{k+1}$ будет иметь ненулевое значение приоритета только относительно одного элемента y_j предыдущего уровня L_k (рис.3). Тогда формула (7) для пересчета приоритетов примет вид:

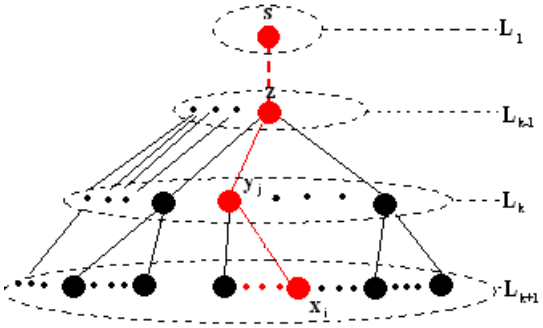

Рисунок 3. Цепь влияния элемента x_i на максимальный элемент иерархии Системы

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

где y_j - это единственный элемент предыдущего уровня иерархии, для которого $w_{y_j}(x_i) \neq 0$. Таким образом, для одного пересчета приоритетов элементов $x_1,..., x_{m_{k+1}}$ потребуется m_{k+1} арифметическая операция. Для того, чтобы вычислить приоритет некоторого элемента x_i построенной иерархической графовой модели ИТС относительно его влияния на Систему в целом, необходимо перемножить приоритеты узлов простой цепи, соединяющей x_i с s, что потребует количества арифметических операций, на единицу меньшего номера уровня иерархии, содержащего x_i.

Полученные приоритеты всех элементов Системы относительно главной цели – совокупной ИТС – представляют из себя весовые коэффициенты вершин графовой модели.

Поскольку все веса графа окажутся меньше или равны единице, для обеспечения положительной полуопределенности его матрицы смежности [7] имеет смысл умножить все коэффициенты на такую константу c, которая приведет весовые коэффициенты к значениям, большим единицы.

4. Моделирование атаки на информационно-технологическую систему. Ответ Системы.

Общение человека с окружающей средой осуществляется через блок датчиков (периферическая нервная система), роль которых в графовой модели ИТС, базирующейся на принципах функционирования НСЧ, выполняют листья [7]. В силу этого любая атака на систему направлена непосредственно на конкретное средство защиты x_i, которому отвечает лист в графе-модели. В общем случае предпринятая атака может либо полностью уничтожить x_i, либо вывести его из строя частично, либо никак не отразится на работе x_i. В последнем случае значение $w(x_i)$ не измениться, в двух других весовой коэффициент атакованного средства очевидно уменьшится.

Уменьшение $w(x_i)$ приведет к возмущению матрицы смежности графа Системы, что, в свою очередь, вызовет возмущение ее СЗ, в некоторых из которых хранится информация, циркулирующая в ИТС [7]. Первоначально матрица смежности графа Системы является положительно полуопределенной [7]. После возмущения ее СЗ данное свойство может быть нарушено. В частности, если $w(x_i)$ станет равным нулю, это обязательно приведет к появлению отрицательного СЗ в матрице смежности графа. Необходимый ответ Системы на атаку должен привести минимальное СЗ матрицы смежности к виду: $\lambda_{\min} \approx 0$, чтобы его знаком можно было пренебречь [7]. Такой результат может быть достигнут за счет увеличения весов неатакованных средств защиты. Модификация весов должна быть проведена в соответствии с установленными выше относительными приоритетами элементов Системы.

Пусть ИТС подверглась некоторой атаке из $\{V_1, V_2, ..., V_l\}$. Пересчитаем весовые коэффициенты всех узлов графа-модели, предварительно изменив количество положительных исходов работы элементов в соответствии с матрицей S и аналогичными матрицами, отвечающими узлам, не являющимися листьями (см. п.3.1). Очевидно, что с выходом из строя некоторого средства защиты, веса оставшихся средств, соответствующие узлы которых не лежат в графе-модели на простой цепи, соединяющей x_i с s, не уменьшатся. Среди имеющихся в распоряжении Системы средств защиты есть как постоянно действующие, так и включаемые при обнаружении попытки нападения. Возрастание весового коэффициента для средств второго типа будет моделировать их активацию.

Таким образом, *ответ* Системы на атаку моделируется путем пересчета весовых коэффициентов элементов Системы, что приводит к активации некоторых средств защиты. Если такой ответ не приведет Систему к виду, для которого $\lambda_{\min} \approx 0$, то ответ Системы недостаточный, необходимо подключение дополнительных средств, не входящих в нее до атаки [7].

Замечание 4. Обнуление или уменьшение $w(x_i)$ приведет к возмущению собственных значений матрицы смежности графа-модели, что вызывает необходимость ответа Системы на предпринятую атаку. Если происшедшие возмущения не каснулись максимальных СЗ, в первоначальных возмущениях которых хранится информация, циркулирующая в Системе [7], или лишь незначительно возмутили их (возмущающее воздействие сравнимо с воздействием шума округлений), то считаем, что информация при атаке не пострадала. В противном случае несанкционированный доступ к информации произошел.

Замечание 5. Если граф Системы имеет достаточно большую размерность, возникает проблема его численной обработки (большое количество арифметических операций для пересчета весов для ответа Системы на атаку). Полезным способом обработки большого числа элементов, попадающих на один уровень иерархии, является объединение их в кластеры (макроузлы) в соответствии с их относительной важностью (таким образом, можно получить кластер самых важных элементов, кластер элементов умеренной важности, а также малой важности) с дальнейшим попарным сравнением относительного воздействия кластеров на соответствующий критерий (элемент) из расположенного выше уровня. После анализа кластеров элементы в каждом из них попарно сравниваются по их относительной важности в этом кластере. Если их слишком много, то они вновь могут быть сгруппированы в пределах кластера.

Замечание 6. Необходимость пересчета весов вершин при моделировании атаки и ответа на нее приводят к динамической модели ИТС. Основное расчетное соотношение (5) принимает вид:

$$A(t)w(t) = \lambda_{\max}(t)w(t), \qquad (10)$$

определяя все составляющие его части как функции времени. Хотелось бы иметь решение задачи (10), выраженное в явном виде через коэффициенты матрицы $A(t)$. Исходя из специфики построения графовой модели, коэффициенты $A(t)$ являются кусочно постоянными функциями на всем промежутке функционирования ИТС, претерпевая разрывы первого рода [16] в точках $t = t_i$, отвечающих времени атаки на Систему или времени ответа Системы на произведенную атаку.

Для получения точного значения $\lambda_{\max}$ необходимо найти корни характеристического многочлена, степень которого равна размерности матрицы $A(t)$. Получить корни многочлена прямыми методами в произвольном случае возможно, когда степень многочлена не превосходит 4 [14]. Если же размерность $A(t)$ больше четырех, то можно снова использовать подход разложения уровней иерархии на кластеры. Для этого для каждого узла $y_j \in L_{k-1}$ множество всех смежных с ним узлов из уровня L_k разбиваем не более, чем на 4 кластера (рис.4). Это приведет к тому, что $\lambda_{\max}(t)$ для матрицы $A(t)$ попарных сравнений воздействия кластеров на соответствующий критерий ($y_j \in L_{k-1}$) можно будет точно выразить через коэффициенты $A(t)$. Дальнейшие действия аналогичны описанным в замечании 5. Очевидно, что для возможности последовательного выражения весов вершин через коэффициенты матриц попарных сравнений количество кластеров, влияние которых исследуется на конкретный элемент иерархии, при разбиении не должно превосходить четырех.

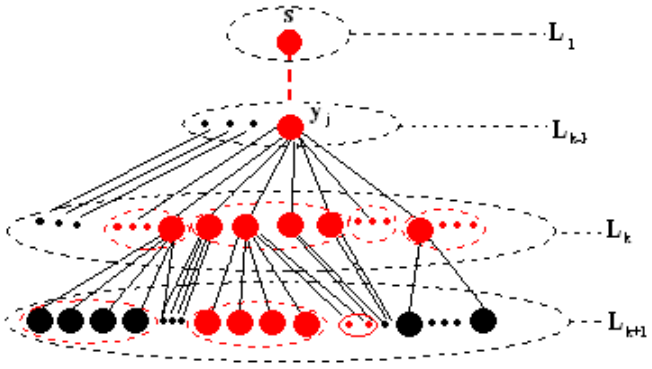

Рисунок 4. Разложение иерархии на кластеры в случае динамической модели Системы.

Решение задачи (10) определит значения весовых коэффициентов вершин графа-модели как функций времени (предполагаем, что $a_{ij}(t)$ известны). Таким образом, матрица смежности графа является динамической, что приведет к возможности получения для нее динамической матрицы возмущения $\Delta(t)$. Очевидно, $\Delta(t)$ - диагональная матрица, для которой диагональные элементы могут иметь различные знаки. Заметим, что диагональные элементы $\Delta(t)$ определяют сдвиг центров кругов Гершгорина [14], в объединение которых находится спектр исходной матрицы смежности (соответствует некоторому начальному моменту времени t_0). Тогда, используя элементы $\Delta(t)$, можно получить грубые оценки для максимально возможных возмущений СЗ матрицы смежности графа-модели, анализ которых предпринимается для оценки результатов атак противника, даже без ее спектрального разложения.

Выводы

1. В работе предложен новый подход к проблеме получения количественных оценок функционирования произвольных элементов ИТС, что не делалось ранее.
2. Предложенный метод вычисления весовых коэффициентов графовой иерархической модели Системы основывается на технике парных сравнений. Подход к парным сравнениям, основанный на решении задачи о СЗ, позволяет обеспечить способ шкалирования при оценке значимости (приоритета) того или иного средства защиты информации по отношению к главной цели построенной иерархии – функционирования совокупной Системы. Кроме того, МАИ, или

метод собственного вектора, обеспечивает измерение согласованности суждений при парных сравнениях, полученных на основе статистических данных.

3. Предложенный способ получения весовых коэффициентов узлов графа-модели, базирующейся на основных принципах функционирования нервной системы человека, дает возможность удовлетворить принципу максимальной начальной приспособленности.
4. Используемый способ вычисления весовых коэффициентов обеспечивает быструю реакцию (ответ) Системы на возмущающее воздействие (атаку), т.к. в силу специфики построенной иерархии, количество арифметических операций для пересчета приоритетов узлов относительно s, как было показано в п.3, невелико. Кроме того, при большой размерности графа-модели это количество можно уменьшить за счет объединения узлов в кластеры.
5. Предлагается способ перехода к динамической модели ИТС, дающий возможность оценки возмущений спектра матрицы смежности графа-модели без построения спектрального разложения за счет использования динамической матрицы возмущений.

Литература.

1. Жданов А.А. Об одном имитационном подходе к адаптивному управлению. Сб. «Вопросы кибернетики». Научный совет по комплексной проблеме «Кибернетика» РАН. М., 1996, с. 171-206.
2. А.А. Жданов. Метод автономного адаптивного управления. – Известия Академии наук. Теория и системы управления, 1999, №5, с. 127-134.
3. Осовецкий Л.Г., Нестерук Г.Ф., Бормотов В.М. К вопросу иммунологии сложных информационных систем. Изв.вузов. Приборостроение. 2003, т.46, №7, с.34-40.
4. Научная сессия МИФИ – 2004. VI Всероссийская научно – техническая конференция «Нейроинформатика - 2004»: лекции по нейроинформатике. – М.: МИФИ, 2004. – 200с.
5. Архипов А., Ишутин А. Применение моделей обнаружения аномалий для выявления атак // Четверта науково-технічна конференція. Правове, нормативне та метрологічне забеспечення системи захисту інформації в Україні. Тези доповідей. – 2006 .- с. 71-72.
6. Хорошко В.А., Терейковский И.А. Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы. – Науково-технічний журнал «Захист інформації». – 2006. - № 3. – С. 57-65.
7. Кобозева А.А., Хорошко В.А. Модель системы защиты информации, основанная на принципах естественной системы управления. – Вісник ДУІКТ. – 2007. - №3. – С.
8. Whyte L.L. Organic Structural Hierarchies, in “Unity and Diversity in Systems”, Essays in honor of L. von Bertalanffy, R.G. Jones and G.Brandl (Eds.), Braziller, New York, 1969.
9. Саати Т. Принятие решений. Метод анализа иерархий. - М.: «Радио и связь», 1993. - 278 с.
10. Андреев В.И., Козлов В.С., Хорошко В.А. Количественная оценка защищенности технических объектов с учетом их функционирования. Науково-технічний журнал «Захист інформації». – 2004. - № 2. – С.47-50.
11. Козлова К.В., Хорошко В.О. Кількісна оцінка захисту радіоелектронних об’єктів. Науково-технічний журнал «Захист інформації». – 2007. - № 1. – С.30-33.
12. Новиков Ф.А. Дискретная математика для программистов. – СПб.: Питер, 2006. – 364 с.
13. Гантмахер Ф.Р. Теория матриц. – М.: Наука. Гл.ред.физ.-мат.лит., 1988. – 552 с.
14. Бахвалов Н.С., Жидков Н.П., Кобельков Г.М. Численные методы. - М.: БИНОМ. Лаборатория знаний, 2006 г.-636 с.
15. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2003. - 501 с.
16. Фихтенгольц Г.М. Курс дифференциального и интегрального исчисления. – М. Наука, 1969.

Вісник ДУІКТ. – 2008. – 6(1). – С. 33-45.