Труды научно-технической конференции кластера пензенских предприятий, обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, с. 38-40 (http://пниэи.рф/activity/science/BIT/T8-p38.pdf)

ИТЕРАЦИОННЫЙ АЛГОРИТМ ПОСТРОЕНИЯ ОПТИМАЛЬНОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ ТКС

Козачок А.И., Левицкая Ю.А. (г. Орел)

Проблему защиты телекоммуникационной системы невозможно решить без грамотно разработанной политики безопасности, под которой понимается совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, регулирующих управление, защиту и распределение ценной информации. Политика безопасности определяется качеством самого документа, который должен соответствовать текущему положению дел в системе и учитывать основные принципы обеспечения информационной безопасности, а также правильность и законченность процесса внедрения. Именно политика безопасности помогает, во-первых, убедиться в том, что ничто важное не упущено из виду, и, во-вторых, установить четкие правила обеспечения безопасности.

Проблема оптимизации политики безопасности практически решена, но необходимо также учесть тот факт, что при неправильном использовании регуляторов безопасности средства защиты будут работать неэффективно. В такой ситуации основной задачей средств защиты информации наряду с обеспечением безопасности становится оценка их целесообразности и эффективности.

На этапе предварительных исследований определяются потребности ТКС в средствах обеспечения безопасности, процессы, используемые в ней в настоящее время, а также политики безопасности средств управления, защищающих эту систему. Далее проводится оценка рисков нарушения информационной безопасности и рассчитываются вероятности возникновения различных видов угроз, для того, чтобы вычислить возможный ущерб от успешной реализации угрозы. Реализация данного этапа невозможна без идентификации для каждой пары «актив - угроза» соответствующих уязвимостей, а также оценки их величин на качественном уровне.

Использование факта, что ущерб определяет последовательность изменения политики безопасности, позволяет непосредственно решить оптимизационную задачу. Довольно часто рассматриваются оптимизационные модели, в которых предполагается полная детерминированность исходных данных, т.е. значения спроса, дохода, затрат и т.п. определяются однозначно. Однако часто значения параметров задачи являются функциями от многих факторов, неучтенных в математической модели, и, с позиций решающего задачу, выступают в роли случайных величин, для которых известны лишь параметры соответствующего распределения вероятностей или другие вероятностные оценки, именно поэтому в данном случае выбор оптимальной политики осуществляется на основе использования марковских процессов, под которыми понимаются случайные процессы, эволюция которых после любого заданного временного параметра t не зависит от эволюции предшествовавшей t, и итерационного алгоритма – обобщенного метода Ховарда. Этот метод позволяет найти оптимальное решение за небольшое число итераций, каждая из которых состоит из двух частей: определение функции цены модели и улучшения решения, причем каждое последующее решение имеет меньшие потери, чем предыдущее.

Суть решения данной задачи состоит в следующем. Имеется управляемая марковская цепь с переоценкой (суммарный средний доход конечен) и конечным множеством состояний $S = \{1,2,...,N\}$, множество политик безопасности $Safe_i = \{1,2,...,k_i\}$ $i \in S$, последовательность решающих функций – стратегий

$\varphi = (f_1, f_2, ..., f_n)$ из пространства $F = U_1 \times U_2 \times ... \times U_N$. Стратегия вида $f^{\infty} = (f, f, ...f, ...)$ называется стационарной. Для каждой решающей функции $f \in F$ заданы $(N \times N)$ – матрица переходных вероятностей $P(f) = \left\| p_{ij}^{Safe} \right\|$, $(i, j \in S)$ и $N \times 1$ – мерный вектор доходов $r(f) = \left[r_i^{Safe} \right]$ (предотвращенный ущерб) с ограничением стоимостных затрат, где $Safe = f(i) \in U_i$. Предполагается, что доход r_i^{Safe} ограничен при всех $i \in S$ и $Safe \in U_i$. Цель управления заключается в максимизации $(N \times 1)$ – мерного вектора суммарных средних доходов на множестве допустимых стратегий $\Phi = \{\varphi\}$, где $P_n(\varphi) = P(f_1)P(f_2)...P(f_n)$, $P_0(f) = 1$ – единичная матрица размера $N \times N$. Стратегия $\varphi^* \in \Phi$ называется β – оптимальной, если при фиксированной величине $\beta \in [0,1)$ $V_\beta(\varphi^*) \ge V_\beta(\varphi)$ для всех $\varphi \in \Phi$, и (β, ε) – оптимальной, если $V_\beta(\varphi^*) \ge V(\varphi) - \varepsilon 1$, для всех $\varphi \in \Phi$, где 1- N – мерный вектор-столбец с компонентами, равными 1. В случае, когда S и U_i конечны, всегда существует стационарная β - оптимальная стратегия.

Введем следующие обозначения и понятия:

$v_i(\beta, f)$ – i -я компонента вектора $V_\beta(f)$;

$\alpha_i(\beta, f)$ – β - прибыль;

$\Delta v_i(\beta, f, s) = v_i(\beta, f) - v_s(\beta, f)$ – относительный β – вес, отвечающий фиксированному состоянию $s \in S$;

$\Delta \alpha_i(\beta, f, s) = \alpha_i(\beta, f) - \alpha_s(\beta, f)$ – относительная β – прибыль, отвечающая фиксированному состоянию $s \in S$.

Итерационный алгоритм Ховарда состоит из двух процедур.

1.Оценивание параметров прибыли. Для каждой стратегии решить систему уравнений

$$w_i + \alpha_s = r_i^{Safe} + \beta \cdot \sum_{j \in S} p_{ij}^{Safe} \cdot w_j, \; i \in S,$$

относительно α_i и w_i, полагая, что $w_s = 0$, $\alpha_s(\beta, f)$ – относительная β – прибыль.

2. Улучшение стратегии. Используя найденные значения w_i, для каждого $i \in S$ выбрать решение $Safe$, обеспечивающее

$$\max_{Safe \in U} \left[r_i^{Safe} + \beta \cdot \sum_{j \in S} p_{ij}^{Safe} \cdot w_j \right] \qquad (1)$$

Здесь если старое решение в i – м состоянии приносит величине критерия (выражению, стоящему в квадратных скобках) столь же большое значение, как и любое другое решение, необходимо оставить старое решение неизменным. Результирующие оптимальные решения $Safe = f(i)$ формируют новую стратегию g. После выполнения операций происходит сравнение используемой стратегии f с полученной g. Если f и g идентичны, то алгоритм заканчивается, и g – β - оптимальная стратегия $A_\beta(g) = [\alpha_i(\beta, g)]$ $i \in S$, является вектором максимальных β – прибылей (величины $\alpha_i(\beta, g)$, $i \in S_S$ определяются по формуле:

$$\alpha_i(\beta, f) = \alpha_s(\beta, f) + (1 - \beta)\Delta v_i(\beta, f, s), \; i \in S_S \qquad (2)$$

В противном случае необходимо положить $f = g$ и осуществить возвращение к оценке параметров. В случае, когда $\beta = 1$ и марковская модель эргодична (при любой стратегии все состояния принадлежат единственному эргодическому классу), система уравнений, представляет собой систему уравнений Ховарда, а приведенный выше метод – итерационный алгоритм Ховарда для процессов с одним эргодическим классом. Обобщенный итерационный алгоритм Ховарда может быть использован для нахождения оптимальных стратегий как для модели с переоценкой, так и для модели без переоценки с одним эргодическим классом.

Марковская модель MA тесно связана с общим марковским процессом принятия решений (при фиксированной стратегии f множество состояний разбивается на несколько эргодических множеств и невозвратное множество, которые могут меняться в зависимости от стратегии f с целевым функционалом)

$$G(f) = \lim_{T\to\infty} \frac{1}{T} \sum_{n=0}^{T-1} P_n(\varphi) r(f_{n+1}) \tag{3}$$

Итерационный алгоритм нахождения стратегии для общей марковской модели $MG = \langle \Phi, G(F) \rangle$ впервые был предложен Ховардом. Блекуэлл доказал существование стационарной 1–оптимальной стратегии модели MA. В дальнейшем Вейнотт предложил итерационный алгоритм нахождения 1-оптимальных стратегий.

В стационарном режиме для любого $f \in F$ справедливо равенство $G(f) = F(f)$. С другой стороны, для любого $\varepsilon > 0$ при достаточной близости β к 1 имеет место неравенство $\left\| A(f) - A_\beta(f) \le \varepsilon \right\|$. Следовательно, при определенных значениях коэффициента переоценки $\beta -$оптимальная стратегия f_β^* модели MA представляет собой $\varepsilon -$оптимальную стратегию f_ε^* общей модели MG. Таким образом, задача нахождения $(1, \varepsilon)$–оптимальной стратегии общей модели MG сводится к нахождению $\beta -$оптимальной стратегии модели MA_β и для ее решения может быть использован обобщенный итерационный алгоритм Ховарда путем выбора значения коэффициента переоценки β в достаточной близости к 1.

Один из путей реализации обобщенного метода Ховарда в нахождении 1–оптимальной стратегии общей марковской модели заключается в последовательном выборе числовых значений коэффициента переоценки $0 < \beta_1 < \beta_2 ... < \beta_n$. Процедура повторяется до тех пор, пока значения относительных $\beta -$весов w_i не будут превышать возможности запоминающего устройства ЭВМ. Таким путем можно строить стратегию, близкую к 1–оптимальной стратегии общей модели. Такой подход позволяет значительно сократить число итераций, где требуется классификация состояний управляемой цепи. Необходимо отметить, что метод последовательного выбора значений β иногда непосредственно может привести к $(1, \varepsilon)$ – оптимальным стратегиям общей модели. Использование приведенного выше алгоритма позволяет на основе рискового подхода получить за конечное число шагов оптимальную политику безопасности, позволяющую эффективно решать задачи защиты информации на основе функционально-стоимостного анализа подсистем защиты ТКС.

Материалы поступили 25.03.2012, опубликовано в Интернет 12.05.2012 по положительной рецензии д.т.н., проф. Малыгина А.Ю. (Пенза).