СЕТЕВАЯ ИНТЕРПРЕТАЦИЯ ЗАДАЧИ ОПТИМИЗАЦИИ ПРОГРАММЫ ДИСТАНЦИОННОГО МОНИТОРИНГА РАБОЧИХ СТАНЦИЙ В СЕТИ КОЛЛЕКТИВНОГО ПОЛЬЗОВАНИЯ

С.Е. Зеленцов
Россия, г. Москва

В.А. Малышев
Россия, г. Шуя

Проблема оценки степени безопасности корпоративной компьютерной сети включает в себя множество аспектов. В частности, если узлы корпоративной сети расположены в разных городах и связаны через интернет, возможен, в том числе, такой подход, как санкционированный взлом серверов баз данных.

В этом случае условно корпоративную компьютерную сеть можно представить в виде многоальтернативного графа, узлами которого являются узловые серверы и серверы баз данных. Попытка взлома имитируется с одного из пользовательских компьютеров по отношению к заданному серверу баз данных. Критерием оценки успешности взлома является прогнозируемый убыток в случае доступа к **j**-му узлу сети за допустимое время. Допустимое время определяется на основании экспертных оценок.

Таким образом задача оценки уязвимости компьютерной сети сводится к нахождению максимального урона за отведённое время, то есть нахождение максимального по длине пути в графе при наложенном ограничении по времени. Под уроном понимается либо стоимость работ по восстановлению информации; либо наносимый ущерб, вызванный утечкой информации, или их совокупность.

Ребру графа предписывается два значения. Первое значение – величина предполагаемого урона в случае вскрытия узла. Второе значение – время на

вскрытие узла, определяемое в ходе экспериментальных исследований или статистических данных.

Анализ графа позволяет выделить пути, приносящие наибольший убыток в случае взлома всех узлов на этом пути за определённый интервал времени.

Другой постановкой задачи является нахождение совокупности путей, потери на которых превышают допустимое значение.

Таким образом, требуется определить путь из вершины **M** графа в вершину **N**, удовлетворяющий следующий условиям:

$$\begin{cases} \sum c_{ij} \to \max \\ \sum t_{ij} \le W \end{cases}$$

где **c** – длина ребра графа, соответствующая возможным потерям; **t** – ожидаемое время на взлом узла; **W –** допустимое время, при превышении которого путь считается безопасным.

Граф описывается тремя матрицами – матрицей инцидентности **S**, матрицей потерь в случае вскрытия узла **P** и матрицей затрат времени на вскрытие узла **T**.

Матрица инцидентности **S** записывается в виде:

$$s_{ij} = \begin{cases} +1, \text{ если } \mathrm{u_j} \text{ исходит из } \mathrm{x_i}; \\ -1, \text{ если } \mathrm{u_j} \text{ заходит из } \mathrm{x_i}; \\ 0, \text{ если } \mathrm{u_j} \text{ не инцидентна } \mathrm{x_i}. \end{cases}$$

где **u** – ребро графа, а **x** – его вершина.

Матрица потерь **P,** элементы которой $\mathbf{p_{ij}}$ соответствуют стоимостным затратам.

Матрица затрат времени **T**, элементы $\mathbf{t_{ij}}$ которой соответствуют ожидаемому времени вскрытия узла **j**.

Для решения задачи выбран алгоритм Дейкстры, программно реализованный в среде Borland Delphi 7.0.