А. М. Цыбулин, А. В. Шипилева (Волгоград, ВолГУ)**. Математическая модель дерева атак на автоматизированную систему.**

Для исследования проблем безопасности и защищенности разрабатываемой автоматизированной системы предлагается использовать модель дерева атак.

В автоматизированной системе имеется достаточно большое количество информационных ресурсов, представляющих интерес для злоумышленников. Для каждого информационного ресурса определяется свое собственное дерево атак. Каждый узел в этом дереве представляет собой некоторую подцель (уязвимость), достижение которой, в случае выполнения ряда условий, позволяет злоумышленнику подняться по дереву на более высокий уровень (до следующей уязвимости) и так до тех пор, пока злоумышленник не достигнет вершины дерева (конечной цели). В последнем случае считается, что злоумышленник успешно реализовал атаку.

Пусть в начальный момент времени $t = 0$ численность целей $Z(0)$ для атак злоумышленника в автоматизированной системе неслучайна, множества целей $Y(0)$ и уязвимостей $X(0)$, ведущих непосредственно к целям, фиксированы. Злоумышленник при положительном воздействии на уязвимости x ($x \in X(0)$) может получить сразу доступ к множеству целей. Однако получить доступ к этим уязвимостям можно только после успешного проведения атак на уязвимости, расположенные на нижних уровнях дерева. Этот процесс можно представить как процесс размножения уязвимостей $X(0)$ и использовать для его описания и исследования модель на базе марковских ветвящихся процессов [I].

В модели предполагается, что воздействия злоумышленника происходят лишь в фиксированные моменты времени $t_k = kT$, $T = \mathrm{const} > 0$, $k \in \mathbf{N}$. Уязвимость x, существуя до момента времени $t_k - 0$, в момент t_k производит $\pi_x^{(k)}$ потомков, где величины $\pi_x^{(k)}$, $k \in \mathbf{N}$, $x \in X$, независимы, одинаково распределены,

$$\mathbf{P}\left\{\pi_x^{(1)} = n\right\} = p_n, \quad \mathbf{E}\,\pi_x^{(1)} = \sum_{n=0}^{\infty} np_n = m < +\infty, \qquad n \in \mathbf{Z}_+.$$

Следовательно, процесс $\xi_x(t)$ роста числа уязвимостей, достижимых из x-уязвимости за время $[0, t]$, определяется формулой

$$\xi_x(t) = \sum_{k=1}^{[t/T]} \varepsilon_x(t_k - 0)\pi_x^{(k)}, \qquad t \geqslant 0, \tag{1}$$

где $[\cdot]$ — целая часть числа.

Считается, что процесс устранения x-уязвимости может происходить как в результате старения (уязвимость устранена путем доработки программного и/или аппаратного обеспечения), так и в результате самолимитирования уязвимостей (уязвимости устраняются проводимой политикой безопасности). Поэтому момент δ_x устранения x-уязвимости определяется следующим равенством:

$$\delta_x = \sigma_x + \min\{l_x, \rho_x\}, \tag{2}$$

где σ_x — момент появления (рождения) x-уязвимости в автоматизированной системе, l_x — продолжительность жизни x-уязвимости до момента гибели вследствие старения, а ρ_x — продолжительность до момента гибели вследствие самолимитирования. Функции распределения этих величин и вероятностей успешных атак на оставшиеся x-уязвимости в модели, в зависимости от применяемых регуляторов безопасности [2], считаются заданными. Исследования проводились численно методом Монте-Карло. Программа модели реализована на языке C–Шарп и имеет удобный для исследователя интерфейс. В докладе приведены результаты построения дерева атак, списка

маршрутов, ведущих к цели (вершине дерева $\langle 0 \rangle$) и значения вероятностей успешных атак для одного из наборов регуляторов безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Харрис Т. Е.* Теория ветвящихся случайных процессов. М.: Мир, 1966, 355 с.
2. *Галатенко В. А.* Оценка безопасности автоматизированных систем. Обзор и анализ предлагаемого проекта технического доклада ISO/IEC PDTR 19791. — Jet info, 2005, № 7 (146).