ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 1
2016

А. В. Ш и п и л е в а (Волгоград, ВолГУ)**. Оценка безопасности компьютерных сетей на основе деревьев атак.**

В современных социально-экономических системах информационные активы являются основным ресурсом и обеспечивают компаниям добавленную стоимость. Сложность и размеры ущерба, вызванного злоумышленными атаками в сети Интернет растут с каждым годом. Для большинства компаний риски информационной безопасности являются наиболее критичными из всего многообразия операционных рисков. От того, насколько эффективно банки, страховые и инвестиционные компании и другие организации управляют этими рисками, зависит их конкурентноспособность и капитализация. В настоящее время большое количество исследований ведется в области разработки систем управления информацией и событиями безопасности [1, с. 57]. Для оценки безопасности компьютерных сетей компаний предлагается использовать модель атаки, построенную на основе деревьев атак.

В 1999 г. Шнейдер предложил использовать деревья атак, которые представляют собой концептуальные диаграммы, описывающие угрозы системе и возможные атаки, направленные на их реализацию. Модель предоставляет возможность для введения оценок каждого шага по некоторым критериям: по времени выполнения, числу операций, оценочной стоимости и т. д. При этом последовательность шагов может быть оценена на основании критериев для каждого шага. Однако эта модель не может быть использована для моделирования атаки, поскольку не обеспечивает средств динамического моделирования, не учитывает решений с различной вероятностью, не обеспечивает выбора следующего этапа на основании результатов предыдущего.

В работе [2, с. 127] была разработана математическая модель злоумышленника, описывающая сетевую атаку на основе марковских ветвящихся процессов, в которой предполагается, что действиям злоумышленника соответствует стохастический алгоритм.

Рассмотрим другой тип атак — коалиционная атака, когда несколько злоумышленников объединяются для достижения цели. При определении вероятности того, что злоумышленник не сможет использовать уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей.

Пусть дерево уязвимостей является m-арным, тогда злоумышленник выбирает для атаки уязвимости с вероятностями $P_0, P_1, \ldots, P_m$, которые определяются из условий [3, с. 77]:

$$0 < P_0 < 1, \quad 0 < P_1 < 1,$$
$$\frac{1}{2}\frac{P_1^2}{P_0} + \frac{1}{2}\Big(\frac{q_1}{q_0} + 1\Big)P_1 < P_2 < \frac{1}{2}\frac{P_1^2}{P_0} + \frac{1}{2}\Big(\frac{q_1}{q_2} + 2\Big)P_1,$$
$$\max\{0, (n+1)\,b_n - a_n\} \leqslant \omega_n \leqslant b_n, \quad n = 2, \ldots, m-1,$$
$$0 < a_2 < P_1, \quad b_2 = P_1(1-\sigma),$$
$$a_n = a_2 - \sum_{k=2}^{n-1} k\omega_k, \quad b_n = b_2 - \sum_{k=2}^{n-1} \omega_k, \quad n = 3, 4, \ldots, m,$$
$$\sigma = -\frac{q_0 P_0}{\alpha P_1}, \quad \alpha = \frac{1}{P_1}\Big(q_0 P_1 + q_1 P_0 - \frac{2q_0 P_0 P_2}{P_1}\Big),$$
$$\omega_n = -\frac{1}{\alpha}\sum_{k=0}^{n} q_k P_{n-k} - (n+1)\sigma P_{n+1} + nP_n - \frac{1}{P_1}\sum_{k=2}^{n-1}(n-k+1)\omega_k P_{n-k+1} \geqslant 0.$$

Действия злоумышленника, находящегося с ним в коалиции описываются заданной инфинитезимальной производящей функцией $g(z) = \sum_{k=0}^{\infty} q_k z^k$. С помощью модели определяются наиболее вероятные маршруты действий злоумышленников, оцениваются риски информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. *Котенко И. В.*, *Саенко И. Б.*, *Полубелова О. В.*, *Чечулин А. А.* Технологии управления информацией и событиями безопасности для защиты компьютерных сетей. — Проблемы информационной безопасности. Компьютерные системы, 2012, № 2, с. 57.
2. *Цыбулин А. М.*, *Шипилева А. В.* Математическая модель злоумышленника в корпоративной сети. — Сборник трудов. Управление большими системами ИПУ им В. А. Трапезникова РАН, 2007, в. 19, с. 127.
3. *Шипилева А. В.* Предельные распределения для ветвящихся процессов с иммиграцией. — Изв. ВУЗов. Математика, 2000, № 1(452), с. 77.