МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗЛОУМЫШЛЕННИКА В КОРПОРАТИВНОЙ СЕТИ

Цыбулин А.М., Шипилева А.В.
(Волгоградский государственный университет, Волгоград)
anatoly.tsybulin@volsu.ru, ashipileva@mail.ru

Для исследования проблем безопасности и защищённости корпоративных сетей предлагается использовать модель действий злоумышленника, построенную на основе марковских ветвящихся процессов. С помощью модели определяются наиболее вероятные маршруты действий злоумышленника и рекомендации по закрытию уязвимых мест.

Ключевые слова: безопасность корпоративных сетей, дерево уязвимостей, ветвящиеся процессы.

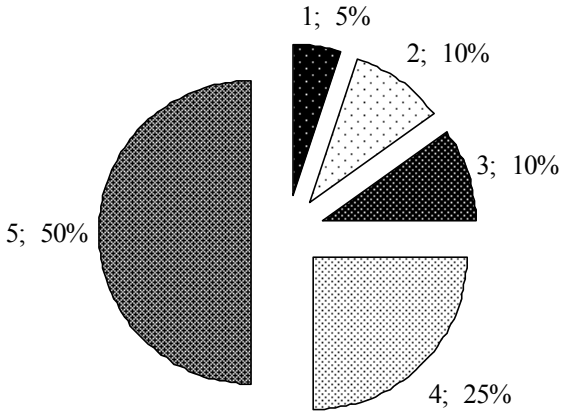
Введение

Многочисленные исследования показывают, что 70-80% всех нарушений в корпоративной сети (КС) приходится на долю внутренних нарушителей. Распределение долей основных источников приведено на рис. 1.

Обеспечение безопасности КС предполагает организацию противодействия любому несанкционированному вторжению в процесс функционирования КС, а также попыткам модификации, хищения, вывода из строя или разрушения ее компонентов, то есть защиту всех компонентов КС – аппаратных средств, программного обеспечения, данных и персонала [2], [4].

Злоумышленник обычно предваряет свои атаки предварительным зондированием всех компонентов КС. На этом этапе он собирает информацию, которая является недоступной для него в рамках служебных полномочий. На практике злоумышленником определяются роли компьютеров в корпоративной сети, выделяются файловые сервера и сервера баз данных, маршрутизаторы и интеллектуальные коммутаторы. На основе этой информации злоумышленником строится дерево уязвимостей КС. И, что

особенно важно, им выбирается инструментарий для проведения атак, например, подбираются эксплойты для осуществления непосредственно атак на узлы корпоративной сети.



1 – внешние нарушения;
2 – корыстные побуждения персонала;
3 – недовольные сотрудники;
4 – стихийные бедствия;
5 – неумышленные действия персонала.

Рис 1. Источники нарушений в современной компании (Источник: Datapro Information Services Group)

1. Основная модель

Для построения математической модели злоумышленника КС используются однородные марковские докритические ветвящиеся процессы [3, 5].

Пусть случайные величины Z_0, Z_1, Z_2, … – число уязвимостей в нулевом, первом, втором, и.т.д. уровнях защиты корпоративной сети, соответствуют числу вершин (состояний) корневого ориентированного дерева уязвимостей (дерева угроз). Дугам дерева уязвимостей приписаны вероятности перехода из состояния i-го уровня защиты в состояние $(i + 1)$-го уровня. Длитель-

ность пребывания в каждом состоянии нулевого, первого, и.т.д. уровнях защиты равна соответственно T_0, T_1, T_2, … .

Если не оговаривается противное, то всегда полагается $Z_0 = 1$ с вероятностью 1 и математическое ожидание количества уязвимостей на первом уровне защиты $EZ_1 < 1$. Обозначим через P вероятностную меру процесса. Распределение вероятностей случайной величины Z_1 определяется числами $P\{Z_1 = k\} = p_k$, $k = 0, 1, 2, \ldots$; $\sum p_k = 1$, где p_k интерпретируется как вероятность того, что уязвимость, существующая на первом уровне защиты, обеспечивает доступ к уязвимостям на втором уровне.

Условное распределение Z_{i+1} при условии $Z_i = k$ определяется из предположения, что разные уязвимости порождают другие уязвимости независимо. Отсюда вытекает, что Z_{i+1} распределена как сумма k независимых случайных величин, каждая из которых распределена так же, как Z_1. Если $Z_i = 0$, то с вероятностью 1 $Z_{i+1} = 0$.

Переходные вероятности рассматриваемого марковского процесса задаются в виде:

$$(1)\ P_{ij}(\tau, t) = P\{Z_{n+1}(t) = j \mid Z_n(\tau) = i\},\ i, j,\ n = 0, 1, 2, \ldots;\ 0 \le \tau \le t.$$

В процессе исследования модели (1) используются прямое и обратное уравнения Колмогорова (2), (3) и определяются распределение вероятностей и моменты случайной величины Z_t; вероятность того, что случайная последовательность $Z_0, Z_1, Z_2, \ldots$ сходится к нулю (злоумышленник не может использовать уязвимости для проведения атак); поведение последовательности в случае, когда она не сходится к нулю, т.е. достигнет ли злоумышленник цели.

$$(2)\begin{cases} \dfrac{\partial P_{ik}(\tau, t)}{\partial t} = -kb(t)P_{ik}(\tau, t) + b(t)\sum\limits_{j=1}^{k+1} P_{ij}(\tau, t)jp_{k-j+1}(t), \\ P_{ik}(\tau, \tau + 0) = \delta_{ik}. \end{cases}$$

Здесь $\delta_{ik} = 1$ при $i = k$, а $\delta_{ik} = 0$ при $i \ne k$.

$$(3)\begin{cases}\dfrac{\partial P_{ik}(\tau,t)}{\partial\tau} = ib(\tau)P_{ik}(\tau,t) - ib(\tau)\sum\limits_{j=i-1}^{\infty} P_{jk}(\tau,t)p_{j-i+1}(\tau), i>0 \\ \dfrac{\partial P_{0k}(\tau,t)}{\partial\tau} = 0, P_{ik}(t-0,t) = \delta_{ik}\end{cases}$$

где $b(t)\Delta + o(\Delta)$ – вероятность, что уязвимость, которая в момент времени t используется злоумышленником для своей атаки, к моменту времени $(t + \Delta)$ завершится успехом. Если уязвимость используется в момент τ, то с вероятностями $p_0(\tau)$, $p_2(\tau)$, $p_3(\tau)$, … злоумышленнику становятся доступны 0, 1, 2, 3, … новых уязвимостей. В соответствии с [5] определяются величины $b_i(t) = i\,b(t)$ и $p_{ij}(t) = p_{j-i+1}(t)$. Часто вместо переходных вероятностей однородного ветвящегося процесса используются соответствующие производящие функции.

Производящая функция однородного ветвящегося процесса имеет вид:

$$(4)\ f(t,z) = \sum_{k=0}^{\infty} p_k(t)z^k, \quad f_i(t,z) = \sum_{j=0}^{\infty} p_{ij}(t)z^j,$$

где $|z| \le 1$ и $p_k(t) = P(Z_t = k)$; с учетом (2) имеет место следующее равенство (5):

$$(5)\quad f_i(t,z) = [f(t,z)]^i.$$

При решении таких задач, как определение моментов величин Z_t или вычисление вероятности того, что злоумышленник не сможет использовать уязвимости для проведения атак за заданное время, необходимо учитывать тип дерева уязвимостей. В исследованиях используются три основных типа: двоичное, троичное и m-арное деревья уязвимостей (могут быть использованы и их комбинации):

- если дерево уязвимостей КС является двоичным, то злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью $p_1 = x$, а правую – с $p_2 = y$. Вероятности x и y выбираются из условий (1):

$$\begin{cases} 0 < x < 1, \\ \dfrac{x(1-x)}{2} < y \le x(1-x). \end{cases}$$

- если дерево уязвимостей КС является троичным деревом, злоумышленник выбирает для атаки уязвимость в левом узле с вероятностью $p_1 = x$, а правую – с вероятностью $p_3 = y$. Вероятности x и y выбираются из условий (1):

$$\begin{cases} 0 < x < 1; \\ 0 < y \le x(1-x)^2, \textit{если } 0 < x \le 1/2; \\ y \le x(1-x)(3-2x)/4, \textit{если } 1/2 < x < 1; \\ y > x(1-x)(2-x)/6, \textit{если } 0 < x \le 2/3; \\ y > x\left(12-12x-x^2\right)/48, \textit{если } 2/3 < x < 6/7; \\ y \ge x(1-x)^2, \textit{если } 6/7 \le x < 1. \end{cases}$$

- если дерево уязвимостей КС является m-арным деревом то злоумышленник выбирает для атаки уязвимости $\{1, 2, \ldots, m; b_1, \ldots, b_m\}$, где $p_1 = b_1$, $p_2 = b_2$, …, $p_m = b_m$, $m \ge 3$ с учётом выполнения следующей системы неравенств [1]:

$$\begin{cases} 0 < b_1 < 1, \\ b_1(1-b_1)/2 < b_2 \le b_1(1-b_1), \\ \max\{0, (n+1)\beta_n - \alpha_n\} \le \nu_n \le \beta_n, n = 2, \ldots, m-1, \end{cases}$$

где $\alpha_1 = b_1(1-\lambda)$, $\beta_1 = b_1(1-\sigma)$,

$$\alpha_n = \alpha_2 - \sum_{k=2}^{n-1} k\nu_k \ , \quad \beta_n = \beta_2 - \sum_{k=2}^{n-1} \nu_k \ ,$$

$$\sigma = \frac{b_1}{b_1^2 + 2b_2} \ , \quad \lambda = b_1\sigma \ , \ n = 3, \ldots, m.$$

Вероятности b_k, $k = 3, 4, \ldots, m$ находятся из равенства [1]:

$$v_k = (k-\lambda)b_k - (k+1)\sigma b_{k+1} - \frac{1}{b_1}\sum_{n=2}^{k-1}(k-n+1)v_n b_{k-n+1}.$$

2. Результаты моделирования

Программа математической модели злоумышленника КС реализована в среде Microsoft Visual Studio.NET 2005 на языке C#. Результаты моделирования действий злоумышленника в КС приведены в экранной копии пользовательского интерфейса модели (см. рис. 2).

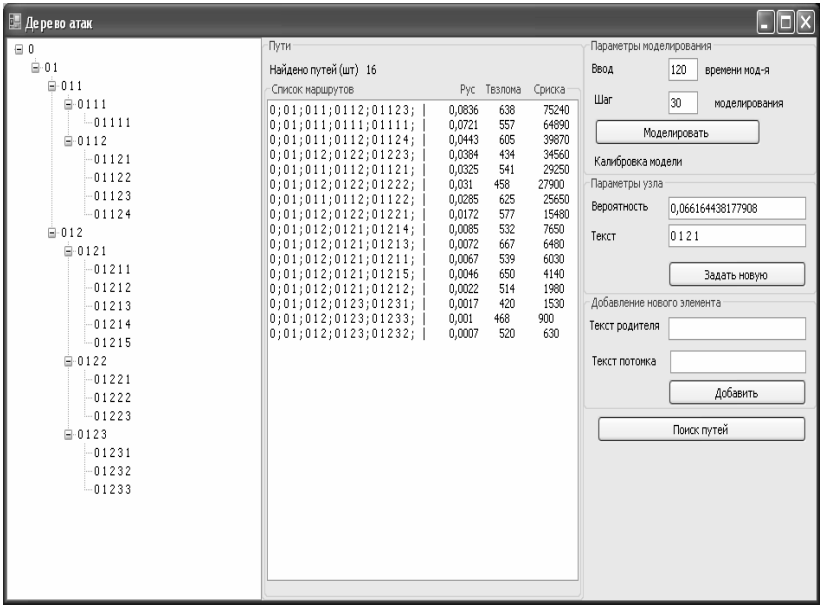


Рис.2. Пользовательский интерфейс модели (экранная копия)

Подсистема защиты КС характеризуется пятью уровнями защиты, корневым деревом уязвимостей Z_0, Z_1, Z_2, Z_3, Z_4, длительности пребывания в каждом состоянии τ_0, τ_1, τ_2, τ_3, τ_4 (задается случайными числами, имеющими равномерное распределение на интервале 0-1000 сек.), располагаемое время для проведения атаки $T_{зад}$ = 800 сек. Стоимость защищаемой информации

составляет 900 000 рублей. Основные результаты: максимальная вероятность достижения злоумышленником цели за $T_{зад,}$: $P_{ус}$ = 0,0836; время, затраченное злоумышленником на достижение цели, $T_{взлома}$ = 638 сек и степень риска составляет $C_{риска}$ = 75 240 руб. На основе этих результатов делаются рекомендации по модернизации средств защиты уязвимостей: 0; 01; 011; 0112; 01123.

Литература

1. ГОРЯЙНОВ В.В., ПОЛКОВНИКОВ А.А. *О предельных распределениях вероятностей для докритических ветвящихся процессов* // Теория вероятностей и ее применение. Т. 41, вып. 2, 1996. С. 417-424.
2. КУРИЛО А.П. и др. *Обеспечение информационной безопасности бизнеса.* ─ М.: БДЦ-пресс, 2005. – 512 с.
3. ПРОХОРОВ Ю.В., РОЗАНОВ Ю.А. *Теория вероятностей*. – М. Изд-во. Наука, 1973. – 395 с.
4. СОКОЛОВ А.В., ШАНЬГИН В.Ф. *Защита информации в распределенных корпоративных сетях и системах.* – М.: ДМК Пресс, 2002. – 656 с.
5. ХАРРИС Т. *Теория ветвящихся случайных процессов.* – М: Мир, 1966. – 355 с.

Статья представлена к публикации
членом редакционной коллегии М.В. Губко