ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 23 МАТЕМАТИКИ Выпуск 1
2016

И. В. Бордак (ФГАОУ ВПО «Северо-Кавказский федеральный ун-т»). **К вопросу оценки вероятности последствий от реализации угроз безопасности информации, циркулирующей в компьютерных системах и сетях.**

Пусть имеется L элементов подсистем автоматизированной информационной системы (АИС). Информация распределена по конечному числу — $N(N \leqslant L)$ элементов подсистем АИС. Тогда для реализации злоумышленником несанкционированного доступа ко всей информации необходимо получить доступ ко всем i-м $(i = 1, 2, \ldots, N)$ элементам подсистем.

Обозначим $P_{\text{дос}}(i)$ — вероятность доступа ко всем i-м $(i = 1, 2, \ldots, N)$ элементам подсистемы АИС, а $P_{\text{раск}}(i)$ — вероятность раскрытия информации злоумышленником в i-х элементах подсистем АИС. Будем полагать, что доступ ко всем i-м $(i = 1, 2, \ldots, N)$ элементам подсистем не зависит от раскрытия информации злоумышленником в i-х элементах подсистем АИС. Тогда с учетом того, что данные события являются независимыми, итоговая вероятность несанкционированного доступа будет иметь следующий вид [2]:

$$P_{\text{нсд}} = P_{\text{дос}}(N) P_{\text{раск}} N. \tag{1}$$

Таким образом, как видно из выражения (1), для определения вероятности — $P_{\text{нсд}}$ необходимо определить $P_{\text{дос}}(i)$ — вероятность доступа ко всем i–м $(i = 1, 2, \ldots, N)$ элементам подсистем АИС и $P_{\text{раск}}(i)$ — вероятность раскрытия информации злоумышленником в i–х элементах подсистем, входящих в АИС.

Для определения вероятности $P_{\text{дос}}$ предположим, что количество элементов подсистем АИС, в которых сосредоточена информация, фиксировано и равно N. Тогда злоумышленник может получить доступ ко всем i-м $(i = 1, 2, \ldots, N)$ элементам подсистем фиксированным количеством способов. Это количество счетное и равно числу перестановок из N элементов, т. е. $N!$ возможных вариантов. Пусть для каждого из k $(k = 1, 2, \ldots, N!)$ способов воздействия имеются векторы $\vec{\lambda}^k = (\lambda_1^k, \lambda_2^k, \ldots, \lambda_{N-1}^k)$ и $\vec{\mu}^k = (\mu_1^k, \mu_2^k, \ldots, \mu_{N-1}^k)$, характеризующие, соответственно, интенсивности прямых и обратных переходов между элементами подсистем АИС. Тогда из множества таких векторов $\vec{\lambda}^k$ и $\vec{\mu}^k$ $(k = 1, 2, \ldots, N!\ )$ можно составить матрицы соответствия [3].

При доступе злоумышленника к какому-либо i –му $(i = 1, 2, \ldots, N)$ элементу подсистема АИС переходит в состояние реализации злоумышленником несанкционированного доступа к i-му $(i = 1, 2, \ldots, N)$ элементу подсистемы. При этом полагая, что переход системы в какое-либо i-е $(i = 1, 2, \ldots, N)$ состояние зависит только от перехода в $i-1$ $(i = 1, 2, \ldots, N)$ состояние и не зависит от других j–х $(j = 1, 2, \ldots, N; i \neq j)$ переходов. Будем полагать также, что событие реализации несанкционированного доступа к i-му $(i = 1, 2, \ldots, N)$ и j-му $(j = 1, 2, \ldots, N; i \neq j)$ элементу подсистем являются несовместными. Тогда, применяя к данному процессу аппарат Марковских случайных процессов и, в частности, цепи Маркова, оценку $P_{\text{дос}}^k(i)$ можно провести, используя выражение для определения финальных вероятностей состояний [1]:

$$P_{\text{дос}}^k(i) = \prod_{j=1}^{i=1} \frac{\lambda_{j,j+1}^k}{\mu_{j,j+1}^k} \left(1 + \sum_{h=1}^{i-1} \prod_{j=1}^{h-1} \frac{\lambda_{j,j+1}^k}{\mu_{j,j+1}^k}\right), \tag{2}$$

где $\lambda^k_{j,j+1}$ и $\mu^k_{j,j+1}$ — интенсивности прямых и обратных переходов между элементами подсистем АИС при использовании злоумышленником k-го $(k = 1, 2, \ldots, N!)$ варианта перехода от одних элементов подсистем к другим.

Для оценки вероятности $P_{\text{раск}}(i)$, воспользуемся методикой, предложенной в [3]. Будем полагать, что информация ограниченного распространения распределена по всем элементам подсистем и при этом часть информации, находящейся в i-м элементе подсистем, не содержится в другом j-м элементе подсистем АИС $(i, j = 1, 2 \ldots, N; i \neq j)$. Тогда, если обозначить $P^i_{\text{раск}}$ — вероятность раскрытия злоумышленником части конфиденциальной информации в i-м элементе подсистем, $1 \leqslant i \leqslant N$, то итоговая вероятность раскрытия всей конфиденциальной информации может быть рассчитана исходя из следующего выражения [3]:

$$P_{\text{раск}} = \prod_{i=0}^{N} \left\{ \left(1 - \max_j \int_0^t e^{-t}(1 - e^{-\mu_j})\, dt\right)(1 - \delta^i) + \max_j \int_0^t e^{-t}(1 - e^{-\mu_j})\, dt\, P^i_{\text{раск}} \delta^i \right\} P_{\text{гр}}. \quad (3)$$

Определив значение $P^k_{\text{дос}}(i)$ по выражению (2), а также $P_{\text{раск}}$ по выражению (3) можно оценить вероятность несанкционированного доступа злоумышленника к информации ограниченного распространения — $P_{\text{ндс}}$, используя выражение (1).

Реализация предложенного метода позволит определить вероятность несанкционированного доступа злоумышленника к защищаемой информации. Собственник информации, в свою очередь, на основании полученных данных будет иметь возможность выявить недостатки в своей деятельности по защите информации и разработать мероприятия, направление на парирование возможных неблагоприятных последствий от реализации злоумышленником различных угроз.

СПИСОК ЛИТЕРАТУРЫ

1. *Тихонов В. И.*, *Миронов М. А.* Марковские процессы. М.: Советское радио, 1997, 488 с.
2. *Росенко А. П.* Методы определения вероятности несанкционированного доступа к конфиденциальной информации. — Докл. Томского гос. ун-та систем управления и радиоэлектроники. Томск: Изд-во ТУСУР, 2012, № 1(25), ч. 2, с. 25–28.
3. *Росенко А. П.* Внутренние угрозы безопасности конфиденциальной информации. Методология и теоретическое исследование. М.: Красанд, 2010, 160 с.