Е.С. Клименко, А.П. Росенко
Россия, г. Ставрополь, Ставропольский государственный университет

МАРКОВСКАЯ МОДЕЛЬ ОЦЕНКИ ВЛИЯНИЯ ВНУТРЕННИХ УГРОЗ НА БЕЗОПАСНОСТЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ[1]

Общие замечания

Марковские случайные процессы получили широкое применение в теории и практике человеческой деятельности. Это связано с возможностью представления и описания достаточно широкого класса прикладных задач конечным множеством возможных состояний. [1]

В [1] показано, что марковские случайные процессы могут быть использованы для оценки влияния на безопасность конфиденциальной информации внутренних угроз. Это связано с тем, что внутренняя угроза является редким, независимым событием, поэтому для исследования ее влияния на автоматизированную информационную систему (АИС), оправдано применение теории марковских случайных процессов, в частности, теория марковских случайных процессов с дискретным параметром. [2,3]

Под внутренней угрозой понимается потенциально-опасное событие, возникающее в процессе функционирования АИС, создающее особую ситуацию. [2,4]

Внутренняя угроза характеризуется следующими особенностями:

– внутренняя угроза может быть преднамеренной (осознанной) или непреднамеренной (неосознанной);

– внутренняя угроза – детерминированное событие, так как связано только с субъектом, а именно, сотрудниками, законными или незаконными пользователями конфиденциальной информации;

– воздействия внутренних угроз на АИС, как правило, являются стохастическими процессами, что дает возможность применять для оценки их воздействия на АИС случайные процессы;

– воздействия внутренних угроз на АИС можно рассматривать как некоторый «шум», накладываемый на процесс функционирования АИС.

Анализ показывает [3], что для оценки влияния внутренних угроз на безопасность конфиденциальной информации, представляется возможным воспользоваться критерием, характеризующим вероятность благополучного исхода от воздействия на АИС внутренних угроз – P_{BY} и вероятность неблагополучного исхода, т.е. $Q_{BY} = 1 - P_{BY}$.

Постановка задачи

Пусть на АИС воздействует n независимых внутренних угроз. При этом очередная внутренняя угроза воздействует на систему только после успешного парирования предыдущей. Процесс перехода системы из состояния в состояние происходит до тех пор, пока она не окажется в поглощающем состоянии, соответствующем реализации злоумышленником внутренней угрозы.

Примем следующие обозначения:

R_i и $\overline{R}_i = 1 - R_i$ – вероятности успешного и неуспешного парирования возникшей i-й внутренней угрозы соответственно;

[1] Работа выполнена при поддержке гранта РФФИ, проект 06-01-00020

q_i и $P_i = 1 - q_i$ – вероятность возникновения и невозникновения i - й внутренней угрозы соответственно;

0, 1, ..., i, ..., n, $n+1$ – состояния, в которых может оказаться рассматриваемая система в результате воздействия n независимых внутренних угроз. При этом состояние $n+1$ соответствует поглощающему состоянию.

Представление АИС в виде графа состояния

Для указанного выше случая граф состояний представлен на рис. 1.

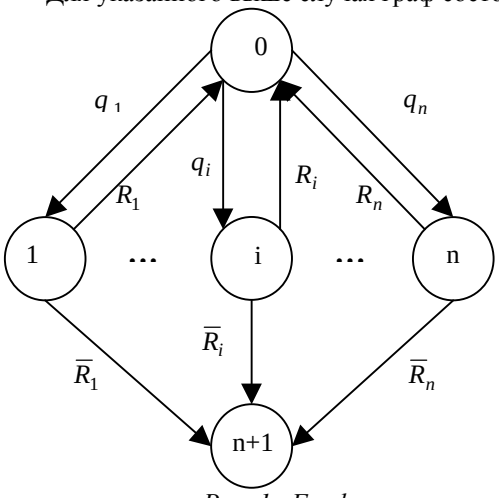

Рис. 1. Граф состояния системы при воздействии на нее n независимых внутренних угроз

Как видно из рис.1, при любом i - м воздействии система может оказаться с вероятностью R_i в исходном состоянии, что соответствует успешному парированию i - й внутренней угрозы доступными методами и средствами. В противоположном случае она с вероятностью $\overline{R}_i = 1 - R_i$ может оказаться в поглощающем состоянии $n+1$, что соответствует реализации злоумышленником i -ой внутренней угрозы.

В соответствии с рис. 1 матрица переходных вероятностей будет иметь следующий вид:

$$\left\| P_{ij} \right\| = \begin{vmatrix} q_{00} & q_1 & \dots & q_i & \dots & q_n & 0 \\ R_1 & q_{11} & \dots & 0 & \dots & 0 & \overline{R}_1 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ R_n & 0 & \dots & 0 & \dots & q_{nn} & \overline{R}_n \\ 0 & 0 & \dots & 0 & \dots & 0 & 1 \end{vmatrix},$$

где $q_{00} = 1 - q_\Sigma$.

Из матрицы следует, что:

– количество единиц в матрице по диагонали соответствует числу поглощающих состояний;

– количество нулей в матрице соответствует числу невозможных переходов.

Частный случай. Воздействие на АИС одной внутренней угрозы

Пусть на автоматизированную информационную систему воздействует одна i - я внутренняя угроза, тогда граф состояния системы, представленный на рис. 1, примет следующий вид (рис. 2).

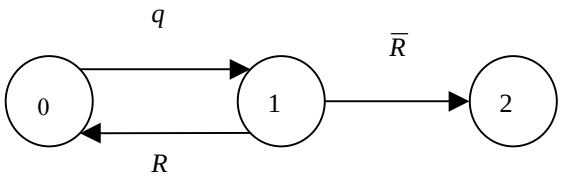

Рис. 2. Граф состояния автоматизированной информационной системы при воздействии на нее одной внутренней угрозы

Исходя из графа и того, что для каждого состояния АИС известны вероятности перехода из одного в другое состояние, матрица вероятностей перехода будет выглядеть следующим образом:

$$\left\| P_{ij} \right\| = \begin{vmatrix} q_{00} & q & 0 \\ R & 0 & \overline{R} \\ 0 & 0 & 1 \end{vmatrix}.$$

Вероятности перехода АИС из одного состояния в другое определяются по формуле полной вероятности вида:

$$P_i(k) = \sum_{j=1}^{k} P_j(k-1) P_{ji} \,, \qquad (1)$$

где k – количество шагов расчета.

Результаты моделирования

Определим вероятность благополучного исхода от воздействия на АИС одной i - й внутренней угрозы в соответствии с выражением (1).

Исходные данные для расчета:

– $P_0(0) = 1$; $P_1(0) = 0$; $P_2(0) = 0$;

–количество шагов расчета $k = 12$;

–в качестве внутренней угрозы принимается кража конфиденциальной информации с электронных носителей, вероятность реализации которой $q_{BУ} = 0{,}658$, тогда вероятность $P_{BУ} = 1 - q_{BУ} = 0{,}342$ [4];

–вероятность парирования ВУ варьируется от $R_1 = 0{,}2$ до $R_4 = 0{,}8$.

Результаты моделирования представлены на рис.3.

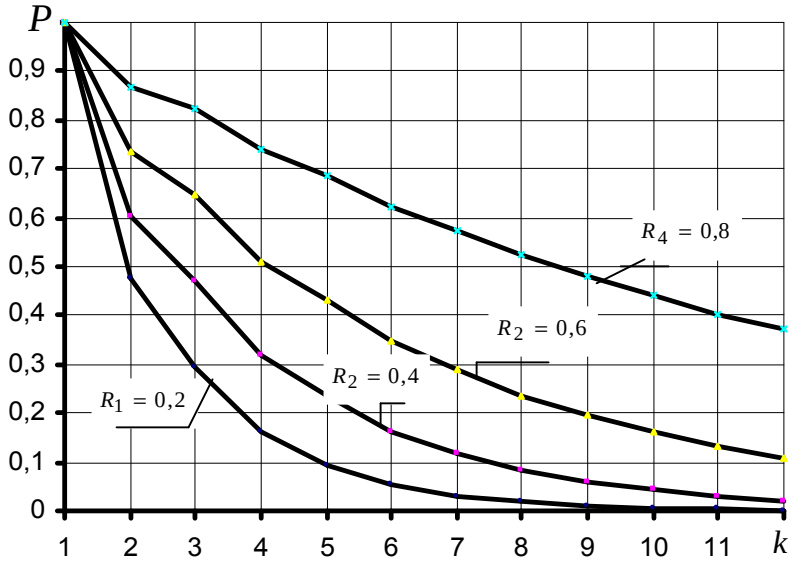

Рис. 3. Результаты моделирования воздействия на автоматизированную информационную систему одной внутренней угрозы

Анализ результатов моделирования, представленных на рис. 3 позволяет сделать следующие выводы:

–после первого шага расчета система не переходит в поглощающее состояние, что соответствует благополучному исходу от воздействия на АИС внутренней угрозы;

–начиная со второго шага расчета, система может попасть в поглощающее состояние, при этом вероятность такого состояния существенно зависит от возможностей по парированию проявившейся внутренней угрозы;

–абсолютная величина изменения вероятности перехода системы в поглощающее состояние возрастает с увеличением количества шагов, что свидетельствует о необходимости совершенствования применяемых защитных механизмов в случае многократного проявления внутренних угроз.

Результаты моделирования могут использоваться для определения наиболее опасных внутренних угроз, последствий их воздействия на АИС, а также разработки организационно-профилактических мероприятий по предупреждению воздействия на автоматизированную информационную систему внутренних угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1.*Росенко А.П.* Модели оценки безопасности конфиденциальной информации с учетом воздействия на автоматизированную информационную систему внутренних угроз//Вестник Ставропольского государственного университета. – Ставрополь: СГУ, 2005. – С. 34–40

2.*Росенко А.П.* Научно-теоретические основы исследования влияния внутренних угроз на безопасность конфиденциальной информации, циркулирующей в автоматизированных информационных системах//Известия ТРТУ. Материалы VII научно-практической конференции «Информационная безопасность». – Таганрог: ТРТУ, 2005. – С. 19–30

3.*Росенко А.П., Клименко Е.С.* О выборе критерия оценки эффективности функционирования системы защиты информации//Первая международная научно-техническая конференция. Инфотелекоммуникационные технологии в науке, производстве и образовании. – Ставрополь: Сев-Кав. ГТУ, 2004. – С. 207–208

4. Внутренние ИТ-угрозы в России 2006. www.infowatch.ru