УДК 658.8

С.С. Ерохин

Оценка эффективности контрмер угрозам информационной безопасности с использованием скрытых марковских процессов

Представлена модель оценки эффективности контрмер угрозам информационной безопасности с использованием скрытых Марковских процессов. Были проведены исследования данной модели на примере организации. Результаты исследование опубликованы в статье.

Вопросы обеспечения информационной безопасности исследуются в разных странах довольно давно. В настоящее время сложилась общая точка зрения на концептуальные основы информационной безопасности. Четко стандартизовать аспекты безопасности впервые было удачно предпринято в Британском стандарте BS7799 «Практические правила управления информационной безопасностью» в 1995 г. Позже этот стандарт переиздан в 2002 г. – ISO1779902. Одним из основных критериев в стандарте ISO1779902 является критерий анализа рисков. Само понятие «анализ рисков» появилось сравнительно недавно и вызывает большой интерес у специалистов в области информационной безопасности.

Анализ информационных рисков [1] – это процесс комплексной оценки защищенности информационной системы (ИС) с переходом к количественным или качественным показателям степени защищенности информационной системы.

Оценка защищенности может проводиться с помощью различных инструментальных средств, а также методов моделирования процессов защиты информации [2].

Так как модели анализа защищенности ИС на данный момент существуют в ограниченном количестве, была предпринята попытка формализации и написания такой модели. В основу данной модели была заложена теория скрытых марковских процессов [3]. При помощи этой теории можно построить граф для ИС, определить вероятности нахождения системы в каком-либо состоянии, при воздействии угроз ИБ, а следовательно, давать рекомендации по повышению уровня безопасности ИС, путем введения контрмер и формировать требования к системе защиты информации.

Модель определения эффективности контрмер угрозам ИБ.

Исходные данные:

1. Множество угроз информационной безопасности $X = \{x_i\}$.

2. Множество контрмер угрозам безопасности $Y = \{y_i\}$.

3. Вектор начального состояния марковского процесса $\bar{a} = (a_0, a_1, \ldots, a_i)$, где i – количество состояний рассматриваемой системы.

4. Матрица переходных вероятностей марковского процесса размерностью $m \times n$:

$$D = \begin{pmatrix} d_{0,1} & d_{0,2} & \ldots. & d_{0,m} \\ d_{1,1} & d_{1,2} & \ldots. & d_{1,m} \\ \ldots. & \ldots. & \ldots. & \ldots. \\ d_{n,1} & d_{n,2} & \ldots. & d_{n,m} \end{pmatrix} \quad (1)$$

5. Интенсивность потока отказа (угрозы ИБ $x_i \in X$) $\lambda = (\lambda_0 \quad \lambda_1 \quad \ldots. \quad \lambda_i)$, причем $\sum_{i=0}^{i} \lambda_i = 1$, где i – количество состояний рассматриваемой системы.

6. Интенсивность потока восстановления (контрмеры угрозам ИБ $y_i \in Y$) $\mu = (\mu_0 \quad \mu_1 \quad \ldots.. \quad \mu_{i-1})$, причем $\sum_{i=0}^{i-1} -\mu_i = 1$, где i – количество состояний рассматриваемой системы.

Алгоритм работы модели:

1. Составляем систему дифференциальных уравнений Колмогорова для марковского процесса по формуле $\frac{dp_i(t)}{dt} = \sum_{j=1}^{n} p_j(t)\lambda_{ji}(t) - p_i(t)\sum_{j=1}^{n} \lambda_{ij}(t)$ и вычисляем вероятность состояний системы в момент времени t без учета интенсивности потока восстановления (контрмер угроза ИБ).

2. Задаем интенсивность потока восстановления μ (контрмеры заданным угрозам).

3. Находим распределение нестационарных вероятностей состояния системы в момент времени (t) [3, 4].

Уравнения Колмогорова составляют систему дифференциальных уравнений и могут быть представлены в следующем виде: $\dot{x} = x \cdot A$, где $x = (x_0(t), x_1(t), \ldots, x_{n-1}(t))$ – вектор-строка, компонентами которой являются неизвестные функции; $\dot{x} = \left(\frac{d}{dt} x_0(t), \frac{d}{dt} x_1(t), \ldots, \frac{d}{dt} x_{n-1}(t) \right)$ – вектор производных функций (градиент); $A = (a_{ij})_{k \times k}$ – квадратная матрица из постоянных коэффициентов.

Решение системы линейных дифференциальных уравнений $\dot{x} = x \cdot A$ удобно выразить через собственные числа $(\upsilon_1, \upsilon_2, \ldots, \upsilon_{k-1})$ и собственные векторы $\left(z^{\langle 1 \rangle}, z^{\langle 2 \rangle}, \ldots, z^{\langle k-1 \rangle} \right)$ матрицы A^T порядка k, тогда решение системы уравнений можно представить в виде $x(t) = \sum_{i=0}^{n-1} b_i e^{\upsilon_i t} (z^{\langle i \rangle})^T$.

Выходные данные:

1. Вектор распределения вероятностей с учетом интенсивностей потока отказов $P_\lambda = (P_1, P_2, \ldots, P_i)$.

2. Вектор распределения вероятностей с учетом интенсивности потока отказов и потока восстановления $P_{\lambda, \mu} = (P_1, P_2, \ldots, P_i)$.

Исследования модели проводились на примере информационной системы, включающей в себя два маршрутизатора, сервер в демилитаризованной зоне и рабочие станции пользователей.

Результаты исследования были обработаны и представлены в виде диаграмм.

Результаты исследования, модели оценки эффективности контрмер угрозам информационной безопасности

Литература

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. М.: Компания АйТи; ДМК Пресс, 2005. – 384 с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД ДС», 2004. – 992 с.

3. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – М.: Наука. Гл. ред. физ.-мат. лит., – 1991. – 384 с.

4. Андронов А.М., Копыткова Е.А., Гринглаз Л.Я. Теория вероятностей и математическая статистика: Учеб. для вузов. – СПб.: Питер, 2004. – 461 с.

Сергей Сергеевич Ерохин
ГОУ ВПО Томский государственный университет систем управления и радиоэлектроники
Инженер кафедры комплексной информационной безопасности электронно-вычислительных систем
Эл. почта: ess@nalog.fisb.ru.

S.S. Erohin

Model assessing the effectiveness of countermeasures to threats information security with the use of hidden Markov processes

In this paper presented a model assessing the effectiveness of countermeasures to threats information security with the use of hidden Markov processes. Studies have been conducted by the example of this model organization. The results of a study published in this article.