УДК 004.056.53

А.П. Росенко

ПРИМЕНЕНИЕ МАРКОВСКИХ СЛУЧАЙНЫХ ПРОЦЕССОВ С ДИСКРЕТНЫМ ПАРАМЕТРОМ ДЛЯ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье обосновывается применение Марковских случайных процессов с дискретными состояниями для оценки информационной безопасности с учетом воздействия на автоматизированную информационную систему различных по природе возникновения внутренних угроз. Представлен граф состояний такой системы, а также математическая модель данного процесса.

Внутренние угрозы; конфиденциальная информация; информационная безопасность; марковские случайные процессы; граф состояний; вероятность.

A.P. Rosenko

APPLICATION OF MARKOV RANDOM PROCESS WITH DISCRETE PARAMETERS FOR ASSESSING OF INFORMATION SECURITY LEVEL

The article substantiates the use of Markov processes with discrete states to assess the information security, taking into account the impact of an automated information system for the different nature of internal threats. The graph of states of such a system, as well as the mathematical model of the process is represented.

Internal threats; confidential information; information security; markov processes; state graph; probability.

1. Актуальность проблемы

Как известно, основными составляющими информационной безопасности любого предприятия являются доступность, целостность, конфиденциальность информации [1]. Анализ показывает, что в большинстве случаев при реализации внутренних угроз (ВУ) сначала нарушается конфиденциальность информации, затем целостность и доступность информации.

В статье рассматривается алгоритм действий злоумышленника по реализации ВУ с целью преодоления защитных механизмов доступности, целостности и конфиденциальности.

2. Постановка задачи

Пусть автоматизированная информационная система (АИС) в результате воздействия ВУ может переходить из состояния в состояние только в фиксированные моменты времени – t_j. Эти моменты времени принято называть этапами Марковского процесса [2].

Так как $T = \{t_j\}$, где $j = \overline{1,\infty}$, то такая последовательность называется цепью Маркова, если для каждого шага вероятность перехода АИС из любого состояния S_i в любое состояние S_j не зависит от того, когда и как она попала в состояние S_i. Состояние перехода АИС из S_i в S_j, состояние тоже является случайным и характеризуется вероятностью P_{ij}.

Можно составить матрицу переходных вероятностей для случая, когда ВУ реализуются в результате преднамеренных или непреднамеренных действий сотрудников. Обозначим нарушение конфиденциальности информации – К, целостности – Ц, доступности – Д. Тогда матрица переходных вероятностей будет иметь следующий вид:

$$P_{ij} = \begin{array}{c} \\ \text{К} \\ \text{Ц} \\ \text{Д} \end{array} \begin{array}{c} \begin{array}{ccc} \text{К} & \text{Ц} & \text{Д} \end{array} \\ \begin{pmatrix} P_{11} & P_{12} & P_{13} \\ P_{21} & P_{22} & P_{23} \\ P_{31} & P_{32} & P_{33} \end{pmatrix} \end{array} \qquad (1)$$

Из матрицы (1) следует:

– вероятности P_{ij} являются условными вероятностями, смысл которых заключается в том, что после *n-го* шага АИС окажется в S_j состоянии, если до этого она находилась в состоянии S_i;

– сумма вероятностей каждой строчки матрицы (1) должна быть равна единице, т.е.

$$\sum_{k=1}^{n} P_{ij} = 1.$$

При наличии исходных данных по условным вероятностям перехода АИС из состояния S_i в состояние S_j можно рассчитать вероятности нарушения конфиденциальности, целостности или доступности в результате воздействия на АИС внутренних угроз.

3. Граф состояний системы

При анализе влияния ВУ на безопасность КИ с использованием Марковского случайного процесса с дискретным параметром удобно пользоваться геометрической схемой – графом состояний, который изображает возможные переходы АИС из S_i в S_j состояние, указанное стрелками [1,2]. Применительно к рассматриваемому случаю граф состояния АИС представлен на рис. 1.

В соответствии с рис. 1 начальное состояние АИС соответствует S_0. Из этого состояния в результате воздействия ВУ она может с вероятностью P_{01} перейти в состояние S_1 и с вероятностью $(1- P_{01})$ – перейти в состояние $\overline{S}_1$. Из состояния S_1 АИС может перейти в состояние $S_к$ с вероятностью $P_{1к}$, характеризующей нарушение конфиденциальности информации и в состояние $\overline{S}_{\hat{e}}$ с вероятностью $1- P_{1к}$, характеризующей соблюдение конфиденциальности информации.

Как видно из рис. 1, из состояния $S_{\hat{e}}$ система может перейти в состояние S_o с вероятностью $P_{кц}$, соответствующей реализации злоумышленником нарушений

целостности информации и в состояние $\overline{S}_{ö}$ с вероятностью *1- $P_{кц}$*, что соответствует соблюдению целостности информации.

Аналогично из состояния $S_{ö}$ система может перейти в состояние $S_{ä}$ с вероятностью $P_{цд,}$ соответствующей нарушению доступности информации, либо в состояние $\overline{S}_{ä}$ с вероятностью *1- $P_{цд,}$* соответствующей соблюдению доступности информации.

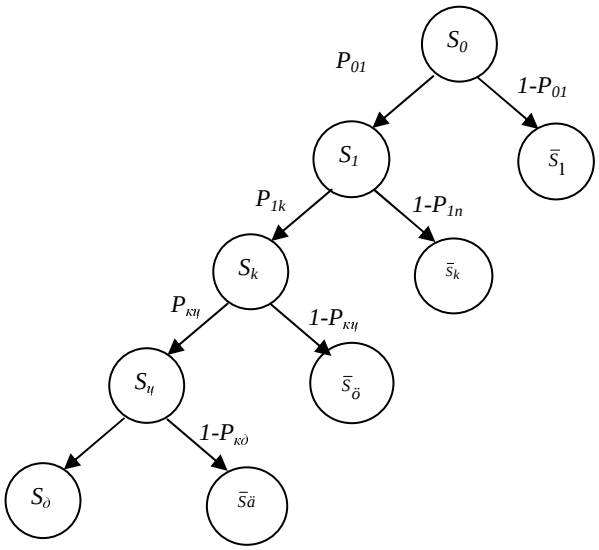

Рис. 1. Граф состояния АИС при воздействии ВУ

4. Аналитические выражения для определения вероятностей благополучного и неблагополучного исхода

Используя полученный граф состояний, представляется возможным получить аналитические выражения для определения вероятностей благополучного и неблагополучного исхода при воздействии на АИС внутренних угроз.

При этом необходимо учитывать то обстоятельство, что воздействие внутренней угрозы на АИС, нарушение конфиденциальности, целостности и доступности информации являются несовместными событиями.

Учитывая данные обстоятельства, вероятность благополучного исхода $P_{б.и.}$ от воздействия на АИС ВУ, в соответствии с рис. 1, будет иметь вид:

$$P_{б.и.} = P_{01} \cdot P_{1к} \cdot P_{кц} \cdot P_{цд}, \qquad (2)$$

а вероятность неблагополучного исхода $P_{н.и}$

$$P_{н.и.} = \prod_{i=0}^{n} P_{0i} \sum_{i=0}^{n} (1 - P_{0i}) . \qquad (3)$$

5. Выводы

Таким образом, как видно из рис. 1, а также из выражений (2), (3) графо-аналитическое представление существенно упрощает процедуру оценки влияния ВУ на безопасность конфиденциальной информации.

При наличии исходной информации, позволяющей определить вероятности благополучного и неблагополучного исхода от воздействия на АИС ВУ, предложенная методика может быть использована для оценки и анализа уровня информационной безопасности предприятий различной формы собственности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Росенко А.П.* Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: Монография – М.: Гелиос АРВ, 2008. – 154 с.

2. *Росенко А.П.* Марковские модели оценки безопасности КИ с учетом воздействия на автоматизированную информационную систему внутренних угроз // Вест. Став. гос. ун-та. – Ставрополь: Изд-во СГУ, 2005. № 43. – С. 34 – 40.

Росенко Александр Петрович
Ставропольский государственный университет.
E-mail: rosenko@stavsu.ru.
355010, г.Ставрополь, ул. Беличенко, 2, кв.21.
Тел.: 8 (8652) 94-13-81.
Заведующий кафедрой компьютерной безопасности.

Rosenko Aleksander Petrovich
Stavropol State University
E-mail: rosenko@stavsu.ru.
App 21, 2, Belichenko str., Stavropol, 355010, Russia.
Phone: 8 (8652) 94-13-81.
Head of the department “Computer Security”.

УДК 681.3.06

А.Ф. Чипига, А.А. Ерещенко, В.С. Пелешенко

МОДЕЛЬ ТРЕХМЕРНОЙ СТРУКТУРЫ ОБЪЕКТОВ С МАТРИЦЕЙ ДОСТУПА

Показан подход к разработке структуры объектов с помощью трехмерной модели представления классов с учетом возможности применения разграничения доступа. Описана модель с дополнительным контролем доступа к объектам на основе классов в объектно-ориентированных системах.

Структура объектов с помощью трехмерной модели представления классов; разграничение доступа; модель с дополнительным контролем доступа к объектам на основе классов в объектно-ориентированных системах.

A.F. Chipiga, A.A. Ereshenko, V.S. Peleshenko

MODEL OF THREE-DIMENSIONAL STRUCTURE OF OBJECTS ACCESS MATRIX