ОЦЕНКА ГОТОВНОСТИ КОМПЬЮТЕРНОЙ СИСТЕМЫ В ПРОЦЕССЕ ВОССТАНОВЛЕНИЯ ПОСЛЕ СЕРИИ АТАК, ПРИВЕДШИХ К ОТКАЗАМ

О.А. Горн[1], А.К. Гуц[1]

[1]Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

ASSESSMENT OF THE READINESS OF THE COMPUTER SYSTEM DURING THE RESTORATION PROCESS AFTER A SERIES OF ATTACKS TO DISCLAIMERS

O.A. Gorn[1], A.K. Guts[1]

[1]Dostoevsky Omsk State University, Omsk, Russia

Аннотация. Рассматривается процедура восстановления компьютерной системы после успешных хакерских атак в рамках теории марковских процессов. Решение уравнений Колмогорова производится с помощью разработанной компьютерной программы.

Abstract. The procedure for restoring a computer system after successful hacker attacks in the framework of the theory of Markov processes is considered. The Kolmogorov equations are solved using the developed computer program..

Ключевые слова: хакерские атаки**,** уравнения Колмогорова, восстановление компьютерной системы.

Keywords: hacker attacks, Kolmogorov equations, computer system recovery.

Любая компьютерная система может отказать при хакерских атаках на нее. Администратор обнаружив «падение» системы, начинает восстановительные работы. Как можно оценить время, которое будет затрачено на восстановление работоспособности системы? А также хотелось бы оценить степень готовности системы в процессе ее восстановления.

Предполагаем, что процесс восстановления состоит из последовательных шагов $i = 0, 1, 2,\ldots, n$, выполняемых один за другим. На шаге i система находится

в состоянии E_i (i = 0, 1, …, n), где E_0 − состояние, с которого начинается восстановление системы. Пусть μ_i = const (i = 0, 1, …, n–1) − интенсивность выполнения i-й операции восстановления системы.

Рассмотрим также состояние E_{01}, которое говорит, что идет форматирование и переустановка операционной системы. Это связано с тем, что в состоянии E_0 администратор убеждается в серьезности повреждений и принимает радикальное решение – «снести всё» и установить операционную систему заново. Соответственно, имеем интенсивность μ_{01} перехода $E_0 \to E_{01}$.

Граф восстановительных работ дан на рис.1.

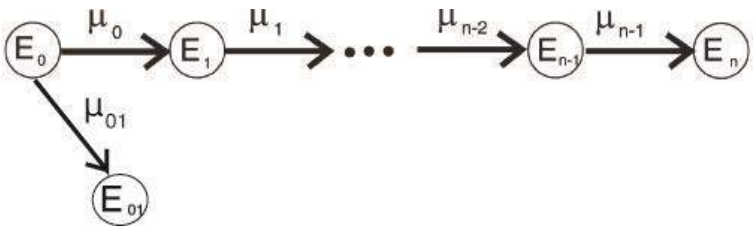

Рис.1. Граф переходов

Очевидно, что среднее время восстановления системы равно

$$T = \frac{1}{\mu_{01}} + \sum_{i=0}^{n-1} \frac{1}{\mu_i}.$$

Пусть $p_i(t)$ − вероятность нахождения компьютерной системы в состоянии E_i (i = 0, …, n) и p_{01} для E_{01}. Тогда процесс восстановления компьютерной системы описывается дифференциальными уравнениями Колмогорова для графа на рис.1 [1, с.128]:

$$p_0' = -(\mu_0 + \mu_{01})p_0(t),$$

$$p_k'(t) = \mu_{k-1}p_{k-1}(t) - \mu_k p_k(t),$$

$$k = 1,2,\dots,n-1, \qquad (1)$$

$$p_n'(t) = \mu_{n-1}p_{n-1}(t),$$

$$p_{01}'(t) = \mu_{01}p_0(t).$$

Под функциональной готовностью $\Gamma(t)$ системы [2] понимаем вероятность того, что система окажется в работоспособном состоянии в произвольно выбранный момент времени после начала ее восстановления (после отказов).

Логично принять, что

$$\Gamma(t) = 1 - [p_{01}(t) + \sum_{i=0}^{n-1} p_i(t)]. \qquad (2)$$

Решая систему (1) с начальными данными $p_0(0) = 1 - p$, $p_k(0) = 0$ ($k = 0, \ldots, n$), $p_{01}(0) = p > 0$ и подставляя найденные вероятности в (2), найдем степень готовности системы $\Gamma(t)$.

Вероятность p находится методом экспертных оценок. Но очевидно, что она имеет небольшую величину, поскольку переустановка операционной системы не является уважаемой процедурой для опытных администраторов.

Разработана компьютерная программа, которая находит $\Gamma(t)$. Данная программа позволяет провести вычислительные эксперименты и определиться, как с адекватностью модели, так и с вероятностью p. Последнее имеет особую актуальность, поскольку, насколько нам известно, никто не проводил социологических исследований, касающихся поведения администраторов в момент выбора – проводить восстановительные работы или переустановить операционную систему.

Список литературы:

1. Венцель Е.С. Исследование операций. М.: Советское радио, 1972. 550с.

2. Потапов В.И. Противоборство технических систем в конфликтных ситуациях: модели и алгоритмы. Омск: Изд-во ОмГТУ, 2015. 168 с.