УДК 004.052

Ю.Л. Поночовный, А.О. Ивасюк

Военный институт телекоммуникаций и информатизации НТУУ «КПИ», Полтава

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ПОТОКОВ ЗЛОНАМЕРЕННЫХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННЫЕ СИСТЕМЫ

В статье рассмотрено построение имитационной модели потока злонамеренных воздействий на информационную систему на основе статистической выборки. При построении модели применен компромиссный вариант совместного использования параметров скоростного и временного распределений. Оценка работоспособности полученного распределения осуществлялась графическим методом с построением вероятностной бумаги.

Ключевые слова: *временное распределение, скоростное распределение, поток злонамеренных действий, анализ Вейбулла, распределение Гумбеля.*

Введение

Постановка проблемы. Современные информационные системы (ИС) представляют собой сложные комплексы взаимосвязанных элементов, функционирующих в условиях влияния большого количества различных внешних воздействий.

Сложность систем и условий окружающей среды обуславливает применение имитационного моделирования для оценки качества ИС. Одной из задач имитационного моделирования является представление потоков случайных событий, описывающих состояния ИС и воздействия на нее.

Так в задачах оценки защищенности и надежности ИС требуется смоделировать потоки злонамеренных воздействий.

Анализ литературных источников. Задачи определения параметров потоков случайных событий, необходимых для построения имитационной модели рассматривались в [2] (для моделирования экспоненциально распределенных потоков), и в [5] (для потоков, имеющих нормальное и вейбулловское распределение). В [7] рассматривается моделирование информационных систем с непуасоновскими входными потоками. Однако анализ статистических данных [4] показывает на отклонение значений параметров потоков злонамеренных воздействий при моделировании их с помощью перечисленных законов распределения.

Таким образом, целью статьи является определение оптимального закона и параметров распределения потоков злонамеренных воздействий на информационные системы, а также построение имитационной модели данных потоков.

Основной материал

1. Определение закона и параметров распределения злонамеренных воздействий на информационные системы. Характеристиками потока случайных событий являются либо параметры временного распределения (случайная величина – время между событиями, параметры – закон распределения, плотность распределения, интенсивность потока) либо параметры скоростного распределения (случайная величина – количество событий за временной интервал, параметры – ведущая функция потока, параметр потока, скоростной закон распределения) [1, 3]. Взаимосвязь между параметрами временного и скоростного распределения описана в [3].

Авторы статьи предлагают использовать комбинированный подход представления параметров потока злонамеренных воздействий, позволяющий достигнуть компромисса между достоинствами и недостатками временного и скоростного распределения. При этом в качестве случайных величин используются время между событиями в потоке и некоторой начальной точкой t0 и количество злонамеренных воздействий на заданном временном интервале.

Для обработки статистической выборки злонамеренных воздействий, зафиксированных в период с 1988 по 2003 год [4] авторы применили математический аппарат анализа Вейбулла [6], реализованный в программном пакете Relex. Результаты поиска оптимального распределения статистической выборки [4] методом максимально вероятностной оценки представлены в табл. 1.

Согласно полученным данным, для статистической выборки [4] оптимальным законом распределения является «Gumbel–» (низкое распределение Гумбеля), плотность и функция распределения которого следующие [8]:

$$f(t) = \frac{1}{\delta}\exp\left[\frac{t-\xi}{\delta} - \exp\left(\frac{t-\xi}{\delta}\right)\right]; \quad (1)$$

$$F(t) = 1 - \exp\left(-\frac{t-\xi}{\delta}\right). \quad (2)$$

Параметры низкого распределения Гумбеля, рассчитанные по статистической выборке [4] для временного интервала 01.01.1988 – 01.11.2003 такие:

– локальность ξ = 122261 (часов);

– масштаб δ = 10557.

Таблица 1

Результаты определения закона и параметров распределения злонамеренных воздействий на информационные системы в программном пакете Relex

Distribution Analysis (Likelihood)		
(Caution: Occurrence Quantity < 20 ... 2-Parameter Weibull = Standard)		
W:Weibull [t0 = None ... 2 parameter]	W:Log Likelihood (LL)= -12168.03	W:=121693 =10,48 Method=RBAmu/intv5
3:Weibull [t0 = -533834.8 ... 3 parameter] [Scale As Recorded]	3:Log Likelihood (LL)= -11618.58	3:=122171 =61,29 Method=RBAmu/t0^/intv5
L:LogNorm [t0 = None ... 2 parameter]	L:Log Likelihood (LL)= -15346.08	L:=114292 =1,181 Method=RBAmu/intv5
N:Normal [t0 = None ... 2 parameter]	N:Log Likelihood (LL)= -13481.35	N:=115728 =15957 Method=RBAmu/intv5
g:Gumbel- [t0 = None ... 2 parameter]	g:Log Likelihood (LL)= -11546.45	g:=122261 =10557 Method=RBAmu/intv5
G:Gumbel+ [t0 = None ... 2 parameter]	G:Log Likelihood (LL)= -16798.1	G:=106550 =22518 Method=RBAmu/intv5
2 Parameter Optimum Distribution: Gumbel- [t0 = None ... 2 parameter]		

На рис. 1 изображена вероятностная бумага низкого распределения Гумбеля, а на рис. 2 – соответствие статистического и эмпирического интегральных законов распределения.

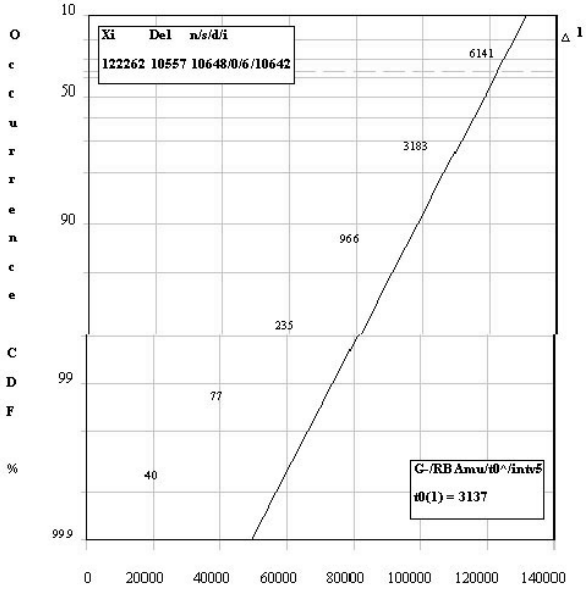

Рис. 1. Вероятностная бумага низкого распределения Гумбеля

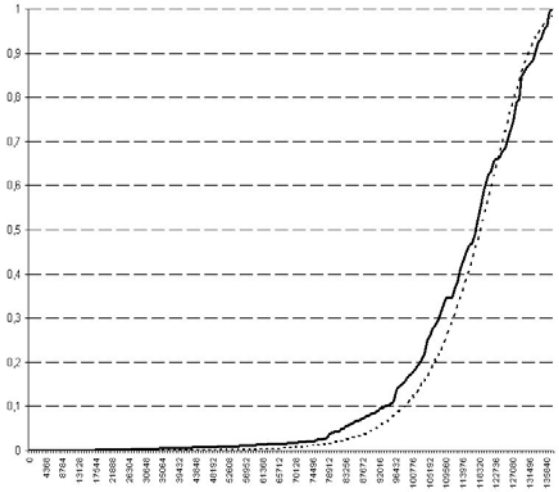

Рис. 2. Статистический и эмпирический интегральные законы распределения

2. Имитационное моделирование потока злонамеренных воздействий на информационные системы. Для имитационного моделирования потока злонамеренных воздействий с функцией распределения F(t), с использованием генератора псевдослучайных чисел, равномерно распределенных в диапазоне (0,1) необходимо получить зависимость, обратную интегральному закону распределения $F^{-1}(t)$. Для низкого распределения Гумбеля такая зависимость существует и выражена законом (3).

$$t = \xi + \delta \cdot \ln\left[-\ln\left(1-R\right)\right], \qquad (3)$$

где R – случайная величина, равномерно распределенная на интервале (0,1). При этом эффективность моделирования и достоверность получаемых результатов, зависят от качества используемых базовых последовательностей R_i псевдослучайных чисел.

Имитационное моделирование потоков случайных событий заключается в получении массива, содержащего моменты времени наступления событий в пределах исследуемого временного интервала. Для существующих имитационных моделей критерием окончания моделирования является:

$$\sum \Delta t_i = \Delta T, \qquad (4)$$

где ΔT – исследуемый временной интервал; Δt_i – моделируемое время между событиями.

В предложенной модели используется другой критерий окончания моделирования:

$$\sum n_{(t_i \in \Delta T)} = N\left(\Delta T\right), \qquad (5)$$

где $\sum n_{(\Delta ti \in \Delta T)}$ – количество злонамеренных воздействий, которые попадают на интервал исследования; $N(\Delta T)$ – случайная величина ожидаемого количества воздействий на исследуемом временном интервале.

Математический аппарат описания случайной величины N(t) выходит за рамки данной статьи, поэтому авторы ограничились гипотезой о том, что N(t) равно максимальному количеству злонамеренных воздействий на исследуемом временном интервале.

Проверка предложенной модели была проведена с использованием редактора Exel, интегральный закон распределения смоделированной статистической выборки представлен на рис. 3.

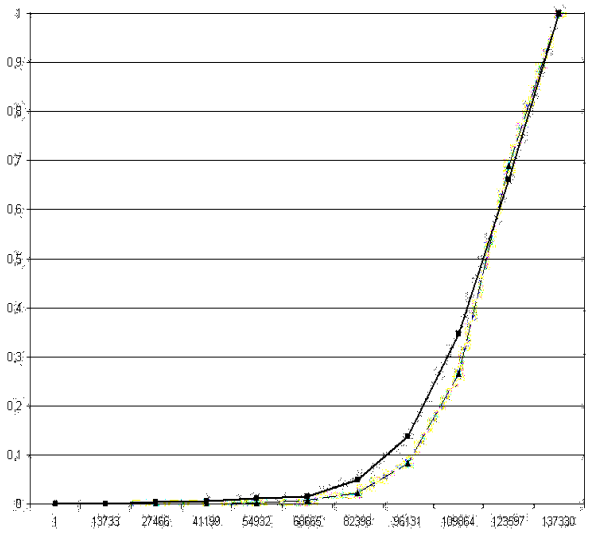

Рис. 3. Статистический и смоделированный интегральные законы распределения

Выводы

В статье рассмотрено построение имитационной модели потока злонамеренных воздействий на информационную систему на основе статистической выборки [4]. При построении модели применен компромиссный вариант совместного использования параметров скоростного и временного распределений. Оценка работоспособности полученного распределения осуществлялась графическим методом с построением вероятностной бумаги.

Из анализа графических зависимостей следует вывод о высокой сходимости результатов натурного и имитационного моделирования.

Предложенную модель рекомендуется использовать для оценки таких показателей качества информационных систем, как защищенность, безопасность и надежность. При этом для определения указанных показателей необходимо использовать либо имитационное моделирование, либо специальный класс аналитических моделей (например [9]), позволяющих учесть изменение интенсивности потока событий, воздействующих на систему.

Список литературы

1. Рыжкин А.А., Слюсарь Б.Н., Шучев К.Г. Основы теории надежности: Учеб. пособие. – Ростов Н/Д: Издательский центр ДГТУ, 2002. – 182 с.

2. Бильчук В.М., Петров В.А. Прикладная математика. Учеб. пособие.– Х.: ХВВКИУРЕ, 1986. – 144 с.

3. Смагин В.А. Техническая синергетика [Электронный ресурс]. – Режим доступа к статье: http://sir35.narod.ru/Cmagin/Contents_26122.htm.

4. ICAT Metabase [Электронный ресурс]. – Режим доступа: http://icat.nist.gov.

5. Имитационное моделирование как метод исследования систем большой сложности [Электронный ресурс]. – Режим доступа: http://ermak.cs.nstu.ru/mmsa/main/Proba.htm

6. Relex Software Help. Weibull Analysis. Copyright © Relex Software Corporation. – 1986-2002.

7. Пономарев Д.Ю. Исследование моделей телекоммуникационных систем с непуассоновскими входными потоками // Современные проблемы радиоэлектроники: Сб. научн. тр.; Под ред. А.В. Сарафанова. – Красноярск: ИПЦ КГТУ. – 2003. – С. 420-425.

8. Поночовный Ю. Л. Определение параметров закона распределения времени между отказами восстанавливаемых обслуживаемых многопользовательских систем с учетом дефектов взаимодействия // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 10 (38). – С.166-174.

9. Одарущенко О.Н. Оценка надежности программно-технических комплексов на основе разработки и исследования многофрагментных марковских моделей // Сб. научн. тр. – Х.: НАН Украины, Петровская академия наук и искусств. – 1997. – Вып. 7. – С. 151-157.

Поступила в редколлегию 29.05.2008

Рецензент: д-р техн. наук, проф. В.С. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ПОТОКІВ ЗЛОВМИСНИХ ДІЙ НА ІНФОРМАЦІЙНІ СИСТЕМИ

Ю.Л. Поночовний, О.О. Івасюк

У статті розглянута побудова імітаційної моделі потоку зловмисних дій на інформаційну систему на основі статистичної вибірки. При побудові моделі застосовано компромісний варіант сумісного використання параметрів швидкісного і тимчасового розподілів. Оцінка працездатності отриманого розподілу здійснювалася графічним методом з побудовою імовірнісного паперу.

Ключові слова: *тимчасовий розподіл, швидкісний розподіл, потік зловмисних дій, аналіз Вейбулла, розподіл Гумбеля.*

SIMULATION MODELING OF MALICIOUS FAULTS STREAMS INFORMATION SYSTEMS

Y.L. Ponochovnyi , A.O. Ivasjuk

In the article the construction of simulation model of stream of the evil-minded affecting is considered informative system on the basis of statistical selection. At the construction of model the compromise variant of sharing of parameters of the speed and temporal distributing is applied. The estimation of capacity of the got distributing was carried out a graphic method with the construction of probabilistic paper.

Keywords: *temporal distributing, speed distributing, stream of evil-minded actions, analysis of Veybull, distributing of Gumbel.*