УДК 004.05

Ю.Л. Поночовный[1], А.В. Боярчук[2], В.С. Харченко[2]

[1] *Полтавский национальный технический университет имени Ю. Кондратюка, Полтава*
[2] *Национальный аэрокосмический университет имени Н.Е. Жуковского "ХАИ", Харьков*

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ВЕБ-СИСТЕМЫ ПРИ АТАКАХ НА УЯЗВИМОСТИ КОМПОНЕНТ И КОНФИГУРАЦИЙ

В статье рассмотрены особенности моделей функционирования веб-системы при атаках на уязвимости. Для трехкомпонентной структуры системы предложена имитационная модель, учитывающая изменение параметра потока атак на доступность сервиса DNS. Указаны особенности построения имитационных моделей, проанализирована сходимость их результатов с аналитическими многофрагментными моделями. Сделаны выводы о возможности применения имитационных моделей при определении оптимального варианта проведения аудитов и обновления функций безопасности системы в процессе ее применения.

Ключевые слова: *имитационная модель, сервис-ориентированные веб-системы, атаки на доступность сервисов.*

Введение

Запуск и эксплуатирование коммерческих веб-сервисов возможны только при условии окупаемости затрат и положительной прибыли. Довольно часто точка окупаемости достигается после введения сервиса в эксплуатацию, а при неправильной оценке рисков вообще может быть не достигнута. Это обуславливает важность моделирования функционирования веб-сервиса с учетом актуальных рисков [1].

Большинство коммерческих веб-сервисов являются наиболее привлекательной целью для проведения атак [2]. В таких условиях актуализируется необходимость моделирования атак на веб-сервис, как событий, обуславливающих его недоступность.

В существующих моделях систем с изменяемыми параметрами используют натурный эксперимент [2], методы имитационного моделирования [3], Байесовские методы исследования [4] и аппарат марковских и полумарковских процессов [5]. Систематизация процесса моделирования (определение множества состояний, переходов между ними, интенсивностей переходов) при использовании аппарата марковских (полумарковских) процессов делает этот подход более предпочтительным.

В случаях, когда построение аналитической модели по определенным причинам усложняется, применяют метод статистических испытаний или метод Монте-Карло, когда вместо описания случайного явления с помощью аналитических выражений, проводится его моделирование процедурой, которая позволяет получить случайный результат. Применение метода статистических испытаний оправдано для сложных систем, которые состоят из большого количества элементов и в которых случайные факторы определенным образом взаимосвязаны. Кроме того, моделирование случайных явлений методом Монте-Карло проводится с целью проверки достоверности результатов, полученных при применении определенного математического аппарата.

Постановка задачи исследования

Современная веб-система является сложной многоуровневой и распределенной. Она может быть представлена с помощью схем различного уровня вложенности. В данной статье рассматривается трехэлементная структурная схема надежности веб-системы (ССН). Она описывает взаимодействие основных служб: присвоения IP-адресов (DHCP), маршрутизации IP-пакетов (Route) и поддержки прямого и обратного преобразования текстовых адресов URL в IP-адреса (DNS). Такое решение обусловлено тем, что согласно классификаторам CVE можно выделить подмножества уязвимостей указанных служб [6]. Это позволяет получить оценки интенсивности атак и их критичности [5]. Неработоспособность любой из перечисленных служб повлечет за собой отказ в обслуживании клиента. На основании этого, ССН будет включать три последовательных элемента, каждый из которых характеризует исправность перечисленных трех служб (рис. 1).

Рис. 1. Структурная схема надежности веб-системы

При оценке готовности веб-систем основное внимание уделяется марковским моделям с учетом отказов и восстановлений аппаратных и программных средств [5, 7]. В [8] анализируется концепция комплексного подхода к гарантоспособности как свойству, объединяющему, в частности, готовность и информационную безопасность. В [9] показана возможность разработки математических моделей, учитывающих недоступность веб-систем, вызванную не только отказами ПС, но и атаками на их компоненты.

Необходимость имитационного моделирования для исследования веб-сервиса как восстанавливаемой обслуживаемой системы, функционирующей в условиях проявления программных дефектов и атак на доступность его компонент, обусловлена следующим [3]:

– необходимостью проверки достоверности результатов, полученных в ходе аналитического моделирования;

– необходимостью разработки подхода к построению имитационных моделей функционирования рассматриваемых систем с целью снятия накладываемых в ходе аналитического моделирования ограничений.

В расчетное время предложенных аналитических моделей невелико (по сравнению с моделями [5]), что позволяет отказаться от разработки сложных альтернативных имитационных моделей веб-серверов. В данной работе целью имитационного моделирования является определение изменения значений функции готовности веб-сервера в процессе эксплуатации системы для случаев проведения атак на службу DNS. По результатам статистических испытаний осуществляется проверка достоверности аналитических моделей.

Особенности построения имитационной модели веб-системы

Анализ задачи имитационного моделирования показал, что с точки зрения формализации рассматриваемый процесс подпадает под класс математических схем систем массового обслуживания (так называемых Q-схем) [10]. Для достижения поставленной цели построение моделирующего алгоритма и последующая его реализация (как и реализация принципов формализации Q-схем) были возложены на модуль имитационного моделирования математического программного пакета MATLAB. В силу ограниченности решаемых задач, пакет визуально-ориентированного программирования SIMULINK не используется, а используются элементы командного окна. Детальное описание команд пакета Mathlab для имитационного моделирования изложено в [10].

В рамках данной работы на базе алгоритма имитационного моделирования (рис. 2) были построены следующие статистические модели веб-систем: с учетом отказов и восстановлений трех служб (ИМ1); с учетом атак на службу DNS с последующим ее перезапуском (ИМ2); с учетом атак на три службы с последующим их перезапуском (ИМ3); с учетом атак на службу DNS с последующим устранением неисправностей конфигурации (ИМ4).

Результаты имитационного моделирования

Результаты сравнения имитационных и аналитических моделей представлены на рис. 3, 4.

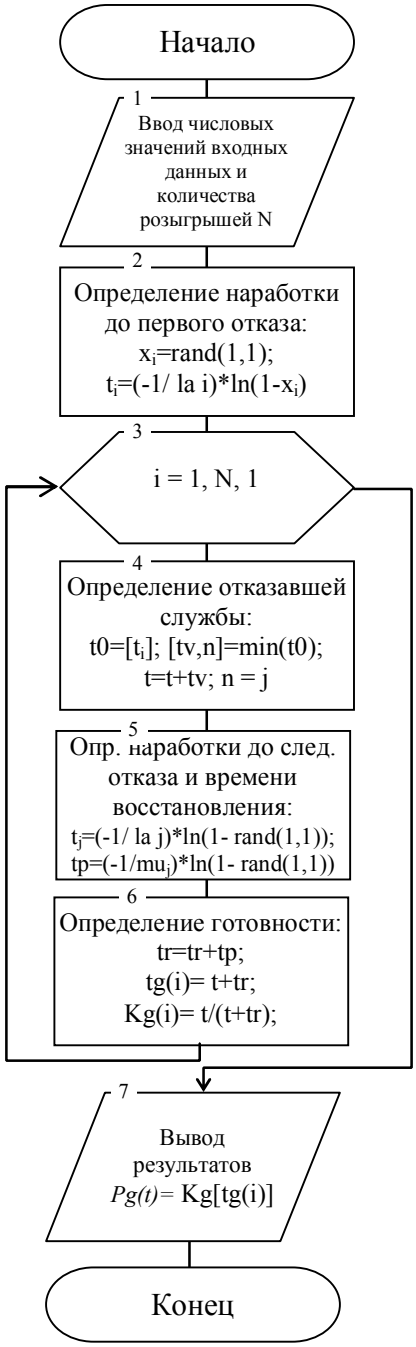
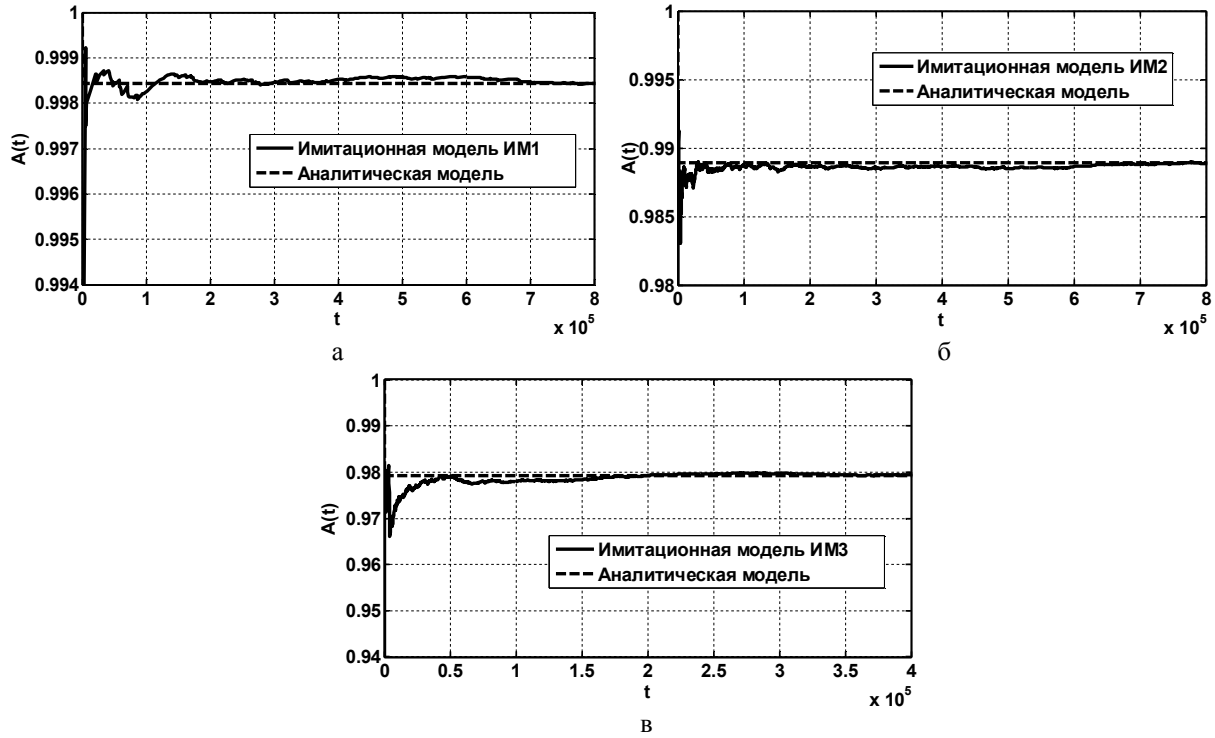


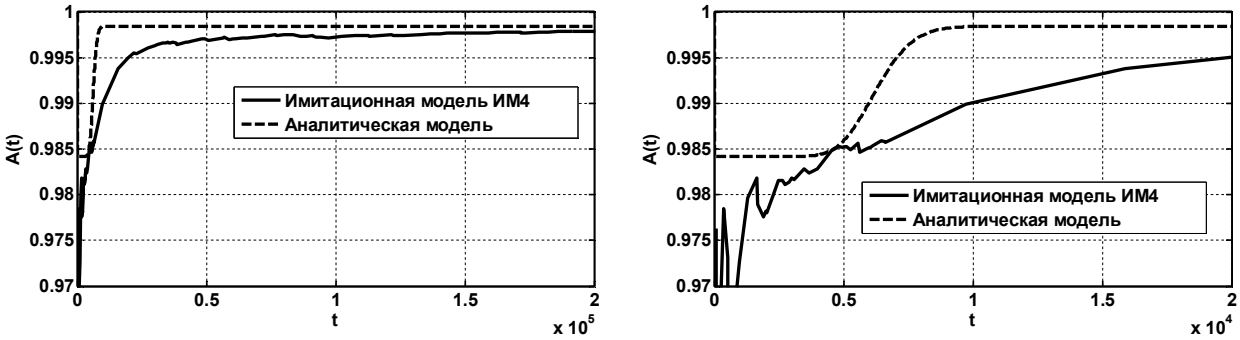
Рис. 2. Алгоритм имитационного моделирования веб-систем

Для приемлемого отображения временной интервал исследования аналитических моделей был специально увеличен на порядок. Как показали результаты испытаний, полученные графики функции готовности имеют характерные фазы развития: переходную на начальном этапе функционирования системы и фазу перехода в установившееся (стационарное) состояние. Для имитационных моделей характерно неоднозначное поведение функции готовности на переходном этапе – на рис. 3, а кривая готовности несколько раз пересекает линию горизонтальной асимптоты устоявшегося значения, а на рис. 3, б, в – подходит к асимптоте снизу.



а б в

Рис. 3. Сравнение результатов имитационного моделирования веб-сервисов и аналитических моделей ИМ1 (а), ИМ2 (б) и ИМ3 (в)



а б

Рис. 4. Сравнение результатов имитационного моделирования веб-сервисов и аналитической модели ИМ4 на временных интервалах [0…200000] часов (а) и [0…20000] часов (б)

Период перехода в устоявшийся режим у функции готовности, полученной с помощью имитационных моделей, составляет $3*10^5$ часов, что на 4 порядка больше, чем у соответствующих аналитических моделей. При этом значения коэффициента готовности в устоявшемся режиме практически совпадают, что подтверждает высокую достоверность аналитических моделей.

Сравнение аналитической и имитационной моделей веб-сервиса с устранением уязвимостей конфигурации (ИМ4) также показало высокую сходимость значений коэффициентов готовности в устоявшемся режиме.

Что характерно, рис. 4, б, имитационная модель в точности повторяет динамику аналитической модели (соответствие примерного выхода кривой готовности из точки минимума после 5000 часов эксплуатации).

Однако видно, что кривая готовности имитационной модели «не успевает» достичь устоявшегося значения в те же сроки, что и аналитическая модель. При этом следует учесть, что для иллюстрации подобного поведения в исходные данные было внесено повышенное количество уязвимостей (nv=30).

Выводы

Анализ результатов моделирования функционирования веб-систем методом Монте-Карло позволяет сформулировать следующие выводы.

1. Применение имитационного моделирования, как и в случае применения многофрагментных моделей, позволяет описать процесс функционирования веб-систем с учетом изменяющихся параметров атак на уязвимости доступности.

2. Применение метода Монте-Карло позволяет ускорить в 1,3 раза определение изменяющихся зна-

чений коэффициента готовности веб-системы при умеренных требованиях к точности моделирования ($\varepsilon>10^{-4}$) и достоверности ($P<0,99$) по сравнению с применением многофрагментного моделирования.

3. Экспериментально подтверждена достоверность результатов, полученных с помощью аналитических многофрагментных моделей функционирования веб-систем. Анализ графиков на рис. 3 и рис. 4 показал, что результаты аналитических и статистических испытаний отличаются не более чем на 6%.

4. Применение имитационных моделей не позволяет в полной мере исследовать поведение функции готовности, а именно точно определить время и значение минимума функции на начальном этапе функционирования системы. Также достаточно сложно выявить тенденцию роста или стационарного режима функции готовности.

Таким образом, результаты имитационного моделирования показали высокую сходимость значений функции готовности в устоявшемся режиме с соответствующими аналитическими моделями. Также было принято решение в дальнейшем отказаться от статистического оценивания функции готовности, так как оно не позволяют однозначно и с заданной точностью определить переходные этапы изменения функции готовности на начальных этапах функционирования.

Планируется включить разработанные имитационные модели в комплексную методику оценки и определении оптимального варианта проведения аудита и обновления функций безопасности веб-систем.

Список литературы

1. Papazoglou M.P. Web Services: Principles and Technology / M.P. Papazoglou // Prentice Hall. – 2007. – Vol. 21. – P. 139-145.

2. Landwehr C. Security Analytics and Measurements / C. Landwehr, G. Cybenko // IEEE Security & Privacy. – 2012. – Vol. 10, no. 3. – P. 5-8.

3. Rotaru T. Service-oriented middleware for financial Monte Carlo simulations on the cell broadband engine / T. Rotaru, M. Dalheimer, F.-J. Pfreundt – Concurrency and Computation: Practice and Experience, John Wiley & Sons, Ltd, 2009 – 348 p.

4. Gashi I. Uncertainty Explicit Assessment of Off-The-Shelf Software: A Bayesian Approach / I. Gashi, P. Popov, V. Stankovic // Elsevier Journal of Information and Software Technology, Elsevier. – 2009. – 51(2). – P. 497-511.

5. Kharchenko V. Web Systems Availability Assessment Considering Attacks on Service Configuration Vulnerabilities / V. Kharchenko, Alaa Mohammed Abdul-Hadi, A. Boyarchuk, Y. Ponochovny // Seria "Advances in Intelligent Systems and Computing". Volume 286. W. Zamojski et al (editors), Springer International Publishing Switzerland, – 2014. – P. 275-284.

6. NVD – Data Feeds. [Электронный ресурс]. – Режим доступа к ресурсу: http://nvd.nist.gov/ download.cfm#XML/

7. Харченко В.С. Базовые многофрагментные макромодели оценки надежности отказоустойчивых компьютерных систем информационно-управляющих комплексов / В.С. Харченко, О.Н. Одарущенко, Е.Б. Одарущенко // Радіоелектронні і комп'ютерні системи. – 2006. – № 5(17). – С. 62-70.

8. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr // IEEE Transactions on Dependable and Secure Computing. – 2004. – Vol. 1. – P. 11-33.

9. Алаа Мохаммед Абдул-Хади. Оценка интенсивности атак на уязвимости доступности коммерческих вебсервисов / Алаа Мохаммед Абдул-Хади // Системи обробки інформації. – Х.: ХУ ПС, 2013. – Вип. 6 (113). – С. 204-208.

10. Дьяконов В.П. MATLAB. Полный самоучитель / В.П. Дьяконов. – М.: ДМК Пресс, 2012. – 768 с.

Поступила в редколлегию 28.04.2015

Рецензент: д-р техн. наук, проф. Б.М. Конорев, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ВЕБ-СИСТЕМИ ПРИ АТАКАХ НА ВРАЗЛИВОСТІ КОМПОНЕНТ І КОНФІГУРАЦІЙ

Ю.Л. Поночовний, А.В. Боярчук, В.С. Харченко

У статті розглянуто особливості моделей функціонування веб-системи. Для трикомпонентної структури системи запропонована імітаційна модель, що враховує зміну параметра потоку атак на доступність сервісу DNS. Визначено особливості побудови імітаційних моделей, проаналізовано збіжність їх результатів з аналітичними багатофрагментним моделями. Зроблено висновки про можливість застосування імітаційних моделей при визначенні оптимального варіанта проведення аудитів та оновлення функцій безпеки системи в процесі її застосування.

Ключові слова: *імітаційна модель, сервіс-орієнтовані веб-системи, оперативна атаки на доступність сервісів.*

SIMULATION MODEL OF WEB-SYSTEM UNDER ATTACKS ON COMPONENT AND CONFIGURATION VULNERABILITIES

Y.L. Ponochovniy, A.V. Boyarchuk, V.S. Kharchenko

The article describes the features of models of functioning web-based system. For a ternary system structure it's proposed simulation model that takes into account the change in the flow parameter attacks on service availability DNS. Peculiarities of simulation models are described; the convergence of the results with an analytical model is analyzed. Conclusions about the possibility of using simulation models in determining the optimal variant of audits and update the security features of the system during its application have been done.

Keywords: *simulation model, service-oriented web-system, attack on the availability of services.*