УДК 004.41:004.056

А.В. Коваленко

Центральноукраинский национальный технический университет, Кропивницкий

МАСШТАБИРОВАНИЕ ИМИТАЦИОННОЙ МОДЕЛИ ТЕХНОЛОГИИ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ

В данной работе разработана и усовершенствована имитационная модель технологии тестирования безопасности на основе положений теории масштабирования имитационных моделей, отличающаяся от известных адаптацией выбора входных операторов управления и данных к повышению требований оперативности разработки и реализации модели, для оценки результатов математического моделирования технологий тестирования безопасности Web-приложений.

Ключевые слова: *имитационная модель, тестирование безопасности, разработка программного обеспечения, уязвимости безопасности.*

Введение

Известным фактом, подтвержденным множеством актуальных результатов исследования, является целесообразность и актуальность проведения имитационного тестирования с использованием компьютерных и телекоммуникационных средств. Для оценки результатов математического моделирования технологий тестирования безопасности Web-приложений разработаем и усовершенствуем имитационную модель. Проведенные исследования показали, что одним из характерных факторов, влияющих на эффективность разрабатываемой имитационной модели, является существенная зависимость от времени реализации и эксперимента. В то же время большинство существующих имитационных моделей обладают рядом недостатков, связанных с излишними затратами вычислительных ресурсов и времени. В случае моделирования в реальном времени это приводит к снижению точности результатов. Поэтому возникает необходимость масштабирования имитационной модели, которое позволило бы снизить вычислительную, алгоритмическую, технологическую или другие виды сложности её анализа без потери точности моделирования поведения на заданном уровне абстракции.

Анализ литературы показал, что в настоящее время существует несколько типичных ситуаций, когда в процессе имитационного моделирования возможно использование операций масштабирования. Например, при проверке свойств, описанных на более высоком уровне абстракции, чем сама модель или при проверке локализованных свойств (например, свойств одного из компонентов большой модели). Проведенные исследования показали, что большинство авторов [1-14] в первом случае, как правило, модель перестраивают вручную на требуемом (более высоком) уровне абстракции. Во втором случае детальные модели компонентов, проверка свойств которых не предполагается или считается избыточной, заменяются на «нулевые компоненты». В дальнейшем для валидации таких упрощенных компонент используются знания экспертов. Одной из основных проблем такого подхода является оценка степени адекватности и возможности таких упрощений. В то же время, как показали исследования динамический выбор достаточного уровня моделирования (степени масштабирования) непосредственно в ходе эксперимента может устранить этот недостаток.

1. Постановка задачи масштабирования имитационной модели технологии тестирования безопасности

Для аргументированного выбора и разработки способа масштабирования проведем анализ существующих подходов и алгоритмов.

Проведенные исследования показали, что в настоящее время существуют различные виды зависимости между операторами имитационной модели. Это транзитивные зависимости по данным и управлению. Данные виды зависимости описаны в литературе [1-8]. В работе предлагается использовать каноническое определение зависимости по данным, связывающей два оператора последовательного процесса с уточнением различия по значению переменной. Также для учета зависимости по управлению предлагается использовать результаты приведеннях работ [6-14] с уточнением, учитывающим зависимости, возникающие при зацикливании участка программы.

Несколько обособленно в списке зависимостей стоят зависимости по времени выполнения, если модельное время выполнения одного из них зависит от модельного времени выполнения другого. При этом нужно учитывать, что не все операторы имитационной модели продвигают модельное время. В работе этим видом зависимости было решено пренебречь, в связи с отсутствием технологической необходимости.

2. Алгоритмы масштабирования имитационной модели технологии тестирования уязвимостей

2.1 Основные определения

Определение 1. Вершина n является родителем некоторой вершины m (потомка) в графе $G = (N, E, n_0)$, если (n,m) ∈ G.E.

Множество всех потомков вершины n в графе G будем обозначать как desc(n,G).

Определение 2. Путём «way» из $n_i \in G.N$ в $n_k \in G.N$ называется последовательность вершин n_i, n_{i+1} ,..., n_k , такая что любые две соседние вершины в ней связаны дугой в графе:

$$(n_j, n_{j+1}) \in G.E,\ j = i, k$$

Запись $n \in$ «way» означает, что вершина n встречается в пути «way».

Определение 3. Путь «way» называется простым, если он состоит из одной вершины [7].

Определение 4. Максимальным называется путь, который бесконечен, либо заканчивается в вершине, не имеющей потомков [7].

2.2 Масштабирование по управлению

В основе масштабирования по управлению лежат постулаты, характеризующие, чувствительность операторов к бесконечному зацикливанию, через понятие максимального пути [7], в терминах последовательных процессов логической схемы имитационной модели.

Определение 5. В графе управления G последовательного процесса p оператор $n_j \in G.N$ прямо зависит по управлению чувствительно к зацикливанию от оператора $n_i \in G.N$ тогда и только тогда, когда у n_i есть два потомка, n_k и n_z , такие что:

1. Во всех максимальных путях, начинающихся с n_k , встречается n_j, и либо $n_i = n_j$, либо n_j строго предшествует любому вхождению n_i.

2. Существует максимальный путь, начинающийся с n_z, такой, что либо в нём не встречается n_j, либо n_i строго предшествует любому вхождению n_j.

В работе [7, 8] приводится обобщенный алгоритм построения графа зависимостей по управлению. Однако, проведенные исследования показали, что для рассматриваемой задачи имитационного моделирования технологии поиска уязвимостей не требуется нахождение прямой зависимости по управлению. Для корректного моделирования рассматриваемого процесса достаточно использовать более слабое понятие транзитивной зависимости по управлению. Это существенно снизит вычислительную сложность алгоритма масштабирования.

На рис. 1 представлена блок-схема алгоритма вычисления транзитивной зависимости по управлению. Следует заметить, что в работе [8] доказана корректность применения транзитивной зависимости по управлению для масштабирования.

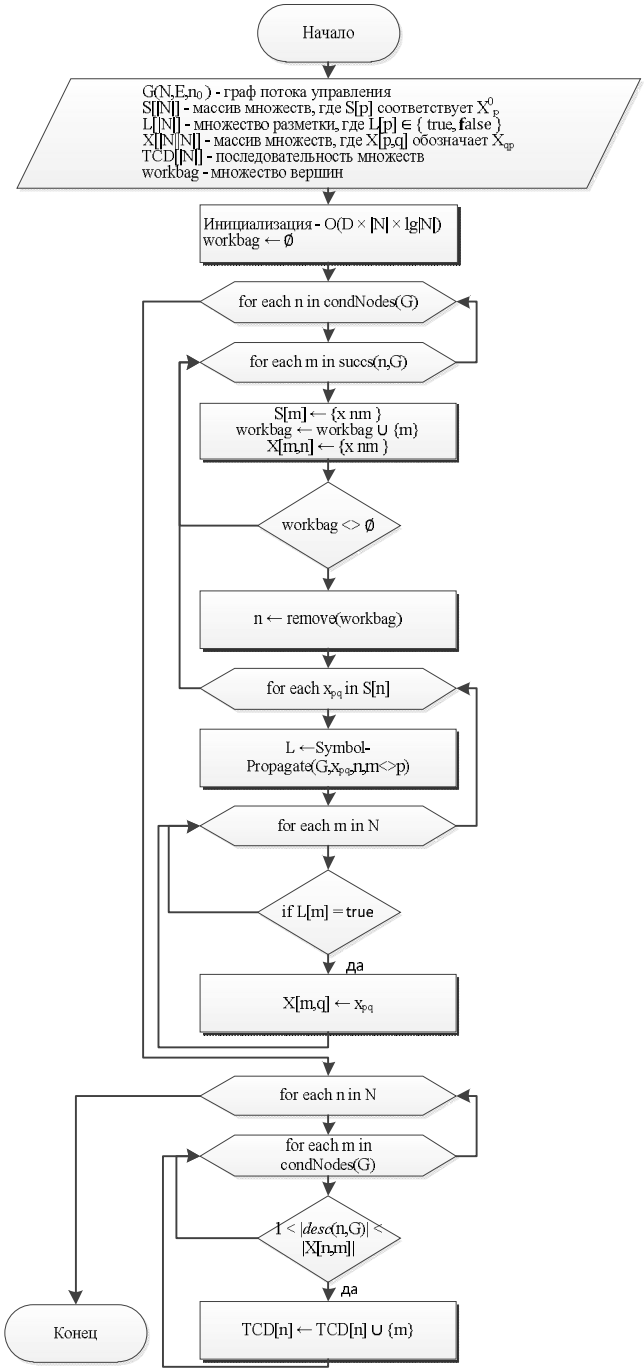

Рис. 1 Блок-схема алгоритма вычисления транзитивной зависимости по управлению

Проведенные расчеты показали, что общая сложность алгоритма равна O(D 2 × |N| 2). Сравнительная оценка предложенного алгоритма с известным алгоритмом, описанным в [7] показала уменьшение сложности за счёт замены цикла по всем управляющим вершинам с множеством символов размера D×|N|.

2.3 Масштабирование по данным

Как уже было указано выше зависимость по данным описывается в работах [7, 8]. В работе используя формализацию известных определений, уточним её указанием переменной, по значению которой возникает зависимость.

Определение 6. В графе управления G последовательного процесса p оператор $n_j \in G.N$ зависит по данным от оператора $n_i \in G.N$ по переменной v тогда, когда существует переменная $v \in p.V_{ar}$, такая что:

1. Существует непростой путь «way» из n_i в n_j, такой что для любого $n_k \in$ «way» $-\{ n_i, n_j \}$[7].

2. $v \in p.def(n_i) \cap p.ref(n_j)$ [7].

На рис. 2 представлена блок-схема алгоритма вычисления транзитивной зависимости по данным.

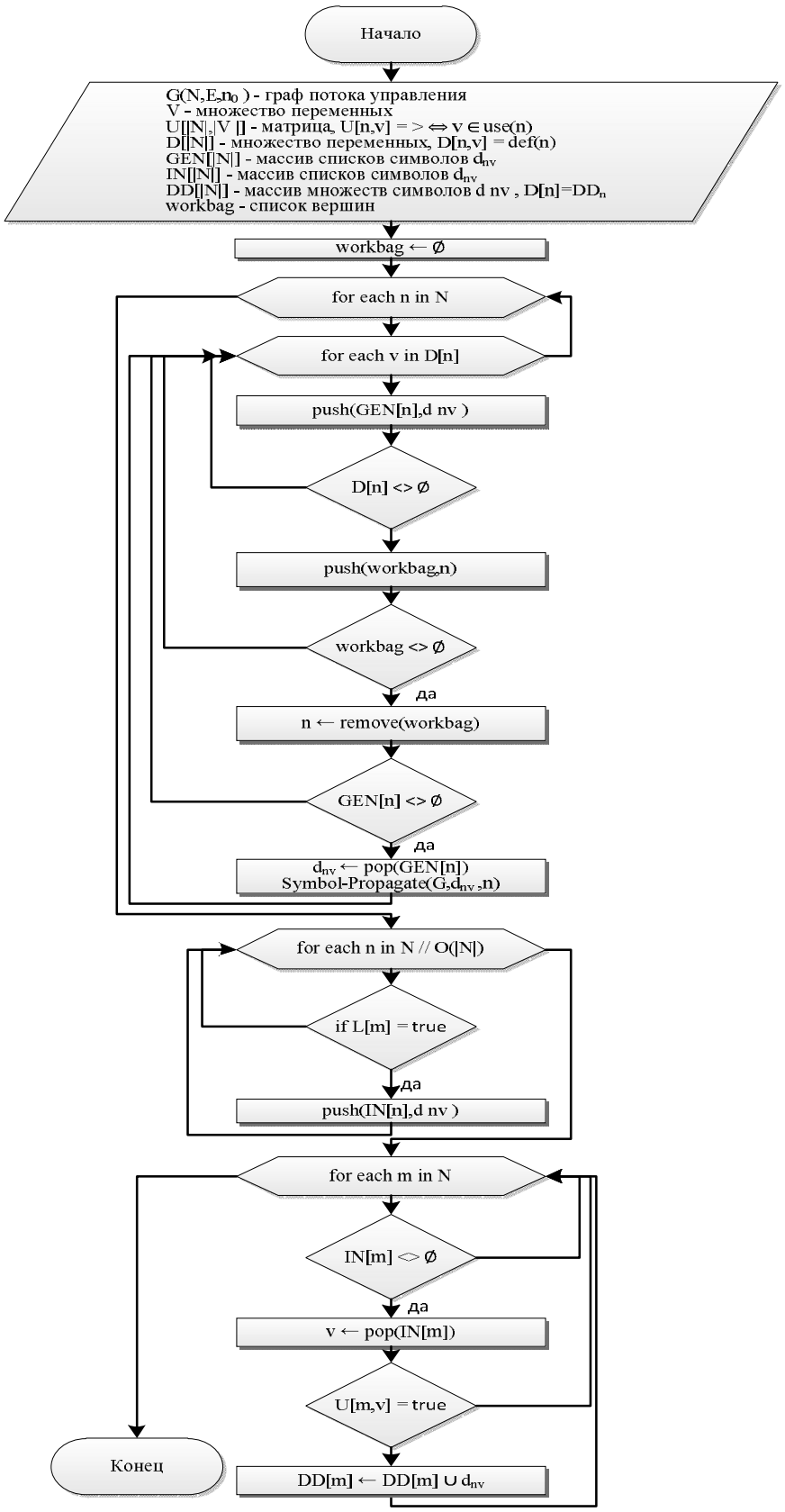

Рис. 2. Блок-схема алгоритма вычисления транзитивной зависимости по данным

Оценка и расчеты вычислительной сложности представленного алгоритма показали, что общая сложность алгоритма составит O(|V | × |N| 2).

Воспользуемся данными алгоритмами для усовершенствования имитационной модели технологии тестирования уязвимостей.

Выводы

В работе получила дальнейшее развитие имитационная модель технологии тестирования безопасности на основе положений теории масштабирования имитационных моделей.

Отличительной особенностью разработанной имитационной модели является адаптация выбора входных операторов управления и данных к повышению требований оперативности разработки и реализации модели, для оценки результатов математического моделирования технологий тестирования безопасности Web-приложений.

Список литературы

1. Maven – Introduction: [Електронний ресурс]. – Режим доступу: https://maven.apache.org/what-is-maven.html.

2. Maven – POM Reference: [Електронний ресурс]. – Режим доступу: https://maven.apache.org/pom.html.

3. Gamma E. Design Patterns: Elements of Reusable Object-Oriented Software. / Erich Gamma. – Reading, Mass. : Addison-Wesley, 1995.

4. Fowler M. Inversion of Control Containers and the Dependency Injection pattern: [Електронний ресурс] / Martin Fowler. – Режим доступу: https://martinfowler.com/articles/injection.html.

5. Spring Framework: [Електронний ресурс]. – Режим доступу: http://projects.spring.io/spring-framework/.

6. Ranganath V., Amtoft T., Banerjee A., Dwyer M., Hatcliff J. A new foundation for controldependence and slicing for modern program structures. Technical report 8, santos lab, Kansas State University, 2004.

7. Савенков К. О. Использование зависимостей при масштабировании имитационных моделей. In Методы и средства обработки информации. Труды второй Всероссийской научной конференции, pages 428–434. - М.: Издательский отдел факультета Вычислительной Математики и Кибернетики МГУ им. М.В. Ломоносова, 2005.

8. Семенов С.Г., Швачич Г.Г., Карпова Т.П., Волнянський В.В. Застосування багатопроцесорних систем для удосконалення технологічних процесів // Зб. наукових праць. Системи обробки інформації. – Х.: ХУ ПС, 2016. – Вип. 3(140) С.221-226.

9. Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко // Збірник наукових праць "Системи обробки інформації". – Випуск 5(142). – Х.: ХУПС – 2016. – С. 153-157.

10. Коваленко А.В. Проблемы анализа и оценки рисков информационной деятельности / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць "Системи обробки інформації". – Випуск 3(140). – Х.: ХУПС – 2016. – С. 40-42.

11. Коваленко А.В. Метод качественного анализа рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 2(23). – Харків: ХУПС. – 2016. – С. 150-158.

12. Коваленко А.В. Метод количественной оценки рисков разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 2 (47). – Харків: ХУПС. – 2016. – С. 128-133.

13. Коваленко А.В. Использование псевдобулевых методов бивалентного программирования для управления рисками разработки программного обеспечения / А.А. Смирнов, А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 1 (37). – Полтава: ПолтНТУ. – 2016. – С. 98-103.

14. Коваленко А.В. Метод управления рисками разработки программного обеспечения / А.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 2 (38). – Полтава: ПолтНТУ. – 2016. – С. 93-100.

Надійшла до редколегії 31.10.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

МАСШТАБУВАННЯ ІМІТАЦІЙНОЇ МОДЕЛІ ТЕХНОЛОГІЇ ТЕСТУВАННЯ БЕЗПЕКИ

О.В. Коваленко

У даній роботі розроблена і вдосконалена імітаційна модель технології тестування безпеки на основі положень теорії масштабування імітаційних моделей, що відрізняється від відомих адаптацією вибору вхідних операторів управління і даних до підвищення вимог оперативності розробки та реалізації моделі, для оцінки результатів математичного моделювання технологій тестування безпеки Web-додатків.

Ключові слова: *імітаційна модель, тестування безпеки, розробка програмного забезпечення, уразливості безпеки.*

SCOPE OF THE IMITATION MODEL OF SAFETY TESTING TECHNOLOGY

O.V. Kovalenko

In this paper, a simulation model of security testing technology has been developed and improved based on the theory of scaling of simulation models, which differs from those known for adapting the choice of input control and data operators to increasing the requirements for the rapid development and implementation of the model, and for evaluating the results of mathematical modeling of Web application security testing technologies.

Keywords: *imitation model, security testing, software development, security vulnerability.*