

УДК 681.321

А.В. Боярчук<sup>1</sup>, А.А. Гордеев<sup>2</sup>, С.Н. Братушка<sup>2</sup>, Р.Н. Головань<sup>2</sup><sup>1</sup> *Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков*<sup>2</sup> *Украинская академия банковского дела Национального банка Украины, Сумы*

## ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ ОЦЕНКИ ГАРАНТОСПОСОБНОСТИ WEB-СЕРВИСОВ

*Определена концепция информационной технологии оценки гарантоспособности Web-сервисов. Проведен анализ существующих инструментальных средств поиска уязвимостей в Web-сервисах. Выполнено описание модулей профилирования, внедрения неисправностей, обеспечения работоспособности Web-сервиса. Сформировано множество неисправностей и их описание.*

**Ключевые слова:** Web-сервис, неисправность, профилирование, сканеры уязвимостей.

### Введение

**Постановка задачи.** Программные комплексы Web-сервисов настоящее время интенсивно применяются при создании широкого спектра критических и бизнес-критических приложений, среди которых можно выделить интернет-банкинг и интернет-коммерцию, уровень надежности которых имеет решающее значение для их владельцев и клиентов.

Некоторые принципы обеспечения гарантоспособности подобных систем сервис-ориентированной архитектуры были проанализированы в работах [1, 2] и других исследованиях.

Было установлено, что практическое внедрение гарантоспособных комплексов должно соответствовать следующим требованиям:

- архитектура системы должна быть построена по COTS-технологии, что предполагает использование коммерческих модулей стороннего производителя для функционирования целевой системы;
- инструментальные средства обеспечения гарантоспособной работы Web-сервиса должны занимать минимальные ресурсы Web-сервера;
- технология обеспечения гарантоспособности должна иметь возможность легко реконфигурироваться для любых систем Web-сервисов, в том числе композитных.

Известны несколько подходов к построению программных модулей для оценки гарантоспособности сервис-ориентированной архитектуры, основанные на методиках внедрения дефектов [3, 4], мониторингах производительности [5, 6] и оценки композитных сервисов [7, 8].

Использование технологии внедрения дефектов является, по нашему мнению, наиболее предпочтительным подходом, поскольку позволяет достаточно гибко моделировать отказы Web-сервисов.

Вместе с тем, реализация этого подхода в Web-сервисах ограничивается рядом причин, связанных,

прежде всего, со сложностью структур и множеством взаимосвязанных уровней Web-сервисов.

**Целью статьи** является разработка информационной технологии (ИТ) оценки гарантоспособности Web-сервисов.

### 1. Концепция информационной технологии

Данная ИТ состоит из трех взаимосвязанных модулей: модуля профилирования, модуля внедрения неисправностей, модуля обеспечения работоспособности Web-сервисов.

Каждый модуль включает соответствующую номенклатуру процедур и инструментальных средств (ИС) (рис. 1).

Схема взаимодействия Web-сервиса с клиентом включает в себя следующие элементы: программное обеспечение (ПО) Web-сервиса, аппаратное обеспечение (АО) Web-сервиса, «последнюю милю» от Web-сервиса до интернет сервис-провайдера, ПО интернет сервис-провайдера, АО интернет сервис-провайдера, «последнюю милю» от ПО и АО клиента, ПО клиента, АО клиента. Предлагаемая ИТ оценки гарантоспособности ориентирована на ПО Web-сервиса.

### 2. Модуль профилирования

Целью функционирования данного модуля является отбор (профилирование) необходимых элементов перед началом использования информационной технологии.

Для достижения цели данным модулем необходимо решить следующие задачи:

- выбор варианта поиска уязвимостей и нахождение уязвимостей в Web-сервисе;
- регистрация найденных уязвимостей;
- выбор объекта внедрения для внедрения неисправностей;
- выбор варианта внедрения неисправностей.

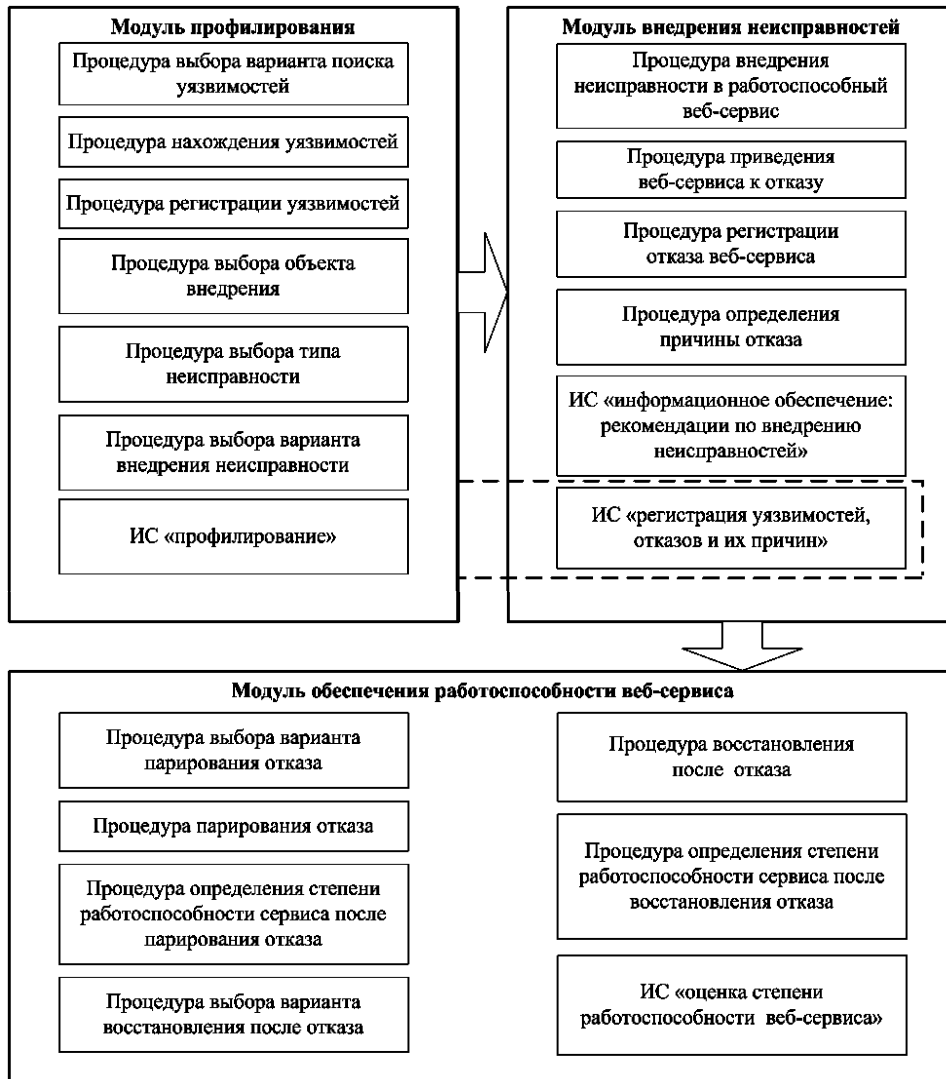


Рис. 1. Структура ІТ

## 2.1. Процедури

*Процедура вибору варіанта пошуку уязвимостей.* Данна процедура основана на виборі необхідного ІС пошуку уязвимостей, т.е. сканера уязвимостей. Вибір повинен здійснюватися на основі наступних критеріїв: пошук уязвимостей в операційній системі (ОС), тип використовуваних протоколів передачі даних, пошук уязвимостей в Web-сервісах, пошук уязвимостей в Web-серверах, пошук уязвимостей в серверах баз даних і серверах додатків. В результаті проведеного аналізу сканерів уязвимостей було встановлено відповідність с критеріями їх вибору (табл. 1).

*Процедура знаходження уязвимостей.* Після того, як визначено перелік ІС пошуку несправностей, необхідно їх застосовувати відповідно до цільового призначення, а саме для пошуку уязвимостей в конкретному Web-сервісі. Для цього необхідно встановити ІС для пошуку уязвимостей,

забезпечити його роботу по необхідному протоколу передачі даних або ж на сервері, на якому знаходиться Web-сервіс, налаштувати його, запустити на виконання і отримати звіт про пошук уязвимостей.

*Процедура реєстрації уязвимостей.* Реєстрація уязвимостей здійснюється кількома способами, залежними від особливостей роботи ІС. Перший варіант базується на аналізі звіту про роботу ІС з метою пошуку уязвимостей. В результаті аналізу звіту перелік уязвимостей реєструється в базі даних. Другим варіантом є реєстрація уязвимостей по факту їх знаходження. Після реєстрації уязвимостей пошук продовжується.

*Процедура вибору об'єкта впровадження.* Данна процедура заключається в виборі безпосереднього об'єкта впровадження несправностей. Об'єкти впровадження повинні відноситися до наступних класів:

- операційна система: Windows, Linux;
- програмне забезпечення: Web-сервіси, Web-сервер, СУБД, сервер додатків.

Таблица 1

Соответствие сканеров уязвимостей критериям их выбора

№	Вариант поиска уязвимости (название ИС)	ОС		Протоколы							ПО			
		Windows	Linux	FTP	SSL	POP3	SMTP	ICMP	SSH	HTTP	Web-сервисы	Web-сервер	Сервер баз данных	Сервер приложений
1	XSpider 7	+	-	-	-	-	-	-	-	+	+	+	+	
2	AWVC	+	-	-	-	-	-	-	-	+	+	-	+	
3	Nmap 4	+	+	+	-	-	-	-	+	+	+	-	+	
4	SSS 7	+	-	+	-	+	+	-	+	+	+	+	+	
5	Nessus 2/3/4	+	+	-	-	-	-	-	-	+	+	-	+	
6	Retina Network Scanner 5	+	-	+	+	+	+	-	+	+	+	+	+	
7	TyphonIII	+	-	-	-	-	-	-	-	+	+	+	-	
8	Nikto	+	+	+	+	-	-	-	-	+	-	+	-	
9	Wikto	+	-	-	-	-	-	-	-	+	-	+	-	
10	Jane-Jane	+	+	-	-	-	-	-	-	+	+	+	+	
11	Httpprint 3	+	+	-	+	-	-	-	-	+	-	+	-	
12	WSFuzzer	-	+	-	-	-	-	-	-	+	+	-	-	
13	WAPT	+	-	-	-	-	-	-	-	+	+	-	+	
14	Sleuth	+	-	-	-	-	-	-	-	+	+	-	-	
15	SIFT	+	-	-	-	-	-	-	-	+	+	-	-	
16	RPVS	+	-	-	-	-	-	-	-	+	+	+	-	
17	Paros	+	+	-	-	-	-	-	-	+	+	+	+	
18	N-Stalker	+	-	-	-	-	-	-	-	+	+	+	-	
19	SMART	+	+	-	-	-	-	-	-	+	+	+	+	
20	ru24_fire	+	+	-	-	-	-	-	-	+	+	+	-	
21	ru24_tools	+	-	+	-	-	-	-	-	+	+	+	-	
22	XSS Tester	+	-	-	-	+	+	-	-	-	+	-	-	

*Процедура выбора типа неисправности.* Предлагаемая процедура заключается в непосредственном выборе типа неисправности, который будет внедряться в объект. Сюда относятся конфигурационные файлы операционных систем, программные инъекции в исходный код Web-сервисов, конфигурационные файлы Web-серверов, SQL-инъекции в базу данных, конфигурационные файлы серверов приложений.

*Процедура выбора варианта внедрения неисправности.* Данная процедура заключается в выборе варианта внедрения неисправностей. Под вариантом внедрения неисправностей подразумевается подмножество ИС из множества ИС – сканеров уязвимостей, которые имеют возможность внедрять уязвимости в объект внедрения.

*ИС «профилирование типов неисправностей».* Данное ИС предназначено для выбора вариантов сканирования уязвимостей Web-сервисов, типов неисправностей, выбора варианта внедрения неисправностей (рис. 2).

### 3. Модуль внедрения неисправностей

Целью функционирования данного модуля является обеспечение внедрения неисправностей в объект внедрения. Здесь решаются следующие задачи:

- внедрение неисправности в Web-сервис;
- приведение Web-сервиса к отказу;
- регистрация отказов Web-сервиса;
- определение причины отказа.

#### 3.1. Формирование множеств неисправностей

На рис. 3 представлено множество неисправностей, включающее подмножества:

- неисправности ПО (1): операционная система сервера, на котором находится Web-сервис, Web-сервер, сервер приложений;
- неисправности сетевого ПО (2): компоненты операционной системы, Web-сервиса, которые участвуют во взаимодействии с сетью;

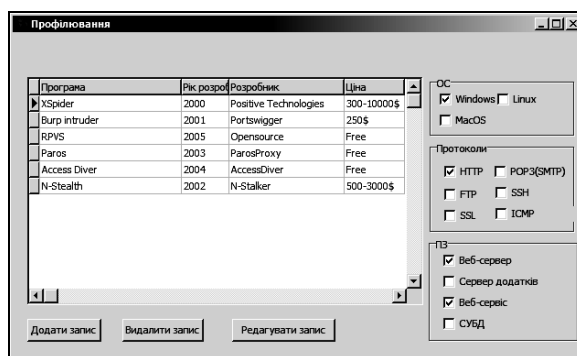


Рис. 2. Экранная форма ИС «профилирование типов неисправностей» – профиль сканеров уязвимостей

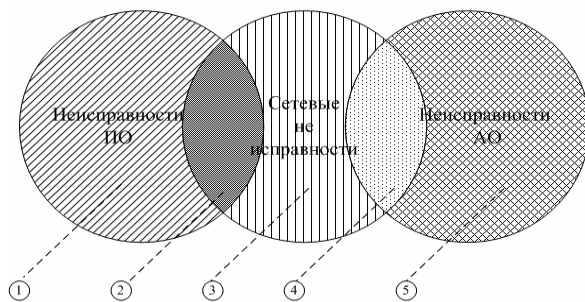


Рис. 3. Множества неисправностей Web-сервисов

- сетевые неисправности (3): протоколы передачи данных;
- сетевые аппаратные неисправности (4): активное сетевое оборудование и пассивное сетевое оборудование;
- неисправности аппаратного обеспечения (5): аппаратное обеспечение (сервер), на котором располагается Web-сервис.

Каждая неисправность с точки зрения внедрения ее в Web-сервис может быть описана множеством из трех элементов: инструментом поиска уязвимостей, инструментом внедрения неисправностей, объектом внедрения:

$$\text{Fault}_i = \{ \text{tool\_vulnerability}_i, \text{object}_i, \text{tool\_infection}_i \}$$

### 3.2. Процедуры

*Процедура внедрения неисправности в работоспособный Web-сервис.* Рассматриваемая процедура заключается в практическом применении ИС для внедрения неисправностей. Она базируется на руководстве пользователя выбранного ИС.

*Процедура приведения Web-сервиса к отказу.* После внедрения неисправности Web-сервис может функционировать до тех пор, пока неисправность не проявится, например, в виде отказа Web-сервиса. В связи с этим существует необходимость приведения Web-сервиса в такое состояние, при котором внедренная неисправность проявится. Для достижения обозначенной цели необходимо сформировать тестовые наборы, выполнение которых приведет к проявлению внедренной неисправности.

*Процедура регистрации отказа Web-сервиса.* Данная процедура заключается в регистрации проявления неисправности в Web-сервисе. Здесь соблюдается следующий принцип: каждый установленный отказ должен быть зарегистрирован. Процедура поддерживается соответствующим ИС «информационное обеспечение: рекомендации по внедрению неисправностей».

*Процедура определения причины отказа.* Процедура заключается в установлении причины отказа Web-сервиса. Причиной отказа может являться не только внедренная неисправность, но и скрытый

дефект, не выявленный при плановом тестировании во время разработки Web-сервиса.

С целью установления истинной причины отказа Web-сервиса предлагается выполнение последовательности действий:

- 1) устраняется неисправность, которая была внедрена в Web-сервис;
- 2) осуществляется тестирование Web-сервиса без неисправности;
- 3) если отказ не проявился при работе Web-сервиса, то считается, что причиной неисправности Web-сервиса являлась внедренная неисправность. В противном же случае, причиной отказа является скрытый дефект.

### 3.3. Инструментальные средства

Рассмотренные процедуры поддерживаются разработанными инструментальными средствами.

*ИС «информационное обеспечение: рекомендации по внедрению неисправностей».* Основной функцией данного ИС является предоставление рекомендаций эксперту по внедрению неисправностей. Эксперт имеет возможность выбора неисправности, в соответствии с которой предоставляется рекомендация по внедрению выбранной неисправности.

*ИС «регистрация отказа и его причины».* Данное ИС предназначено для регистрации установленного отказа и его причины. Рассматриваемое ИС поддерживает следующие функции: добавление информации об отказе, удаление записи об отказе, редактировании записи об отказе.

## 4. Модуль обеспечения работоспособности Web-сервиса

Цель функционирования данного модуля заключается в обеспечении работоспособности Web-сервиса при проявлении в нем неисправности. Для достижения обозначенной цели в рамках использования данного модуля решаются следующие задачи:

- выбор варианта парирования отказа;
- парирование отказа;
- восстановление после отказа;
- определение степени работоспособности Web-сервиса после отказа.

### 4.1. Процедуры

*Процедура выбора варианта парирования отказа.* Данная процедура выполняет выбор варианта парирования отказа Web-сервиса. К вариантам парирования можно отнести мажорирование, дублирование и резервирование.

*Процедура парирования отказа.* Предлагаемая процедура заключается в определении результативности применения вариантов парирования отказов Web-сервисов.

*Процедура определения степени работоспособности сервиса после парирования отказа.* Данная процедура заключается в определении степени работоспособности Web-сервиса. Степень работоспособности Web-сервиса в данном случае определяется множеством выполняемых API-функций из общего числа функций.

*Процедура выбора варианта восстановления после отказа.* Цель данной процедуры заключается в выборе мероприятий по восстановлению Web-сервиса. К мероприятиям восстановления Web-сервисов относятся:

замена отказавшего компонента,  
повторная установка компонента ПО,  
восстановление хранимых данных,  
восстановление данных сессии,  
замена отказавшего компонента,  
перезапуск среды окружения,  
повторная установка среды окружения ПО,  
восстановление хранимых данных,  
перезапуск Web-сервисов,  
повторная установка приложения,  
перезапуск приложения.

*Процедура восстановления после отказа.* Процедура заключается в применении мероприятий по восстановлению Web-сервиса.

*Процедура определения степени работоспособности сервиса после восстановления отказа.* Аналогично процедуре определения степени восстановления после парирования отказа.

### Заключение

В данной работе предложена концепция ИТ оценки работоспособности Web-сервисов. Для решения поставленной задачи был проведен анализ ИС нахождения уязвимостей по внедрению неисправностей, разработаны модуль профилирования, модуль внедрения неисправностей и модуль обеспечения работоспособности, описаны способы практической реализации данной технологии.

В дальнейшем методы и инструментальные средства могут использовать эксперты при прове-

дении независимой верификации, аудите для оценки качества систем Web-сервисов бизнес-критического применения на различных этапах жизненного цикла.

Будущие экспериментальные исследования будут направлены на разработку инструментальной поддержки предлагаемой технологии и ее апробацию.

### Список литературы

1. Khan Khaled M. *Managing Web Service Quality: Measuring Outcomes and Effectiveness.* / Khaled M. Khan. – IGI Global, 2008. – 418 p.
2. Menaske D. *Productivity of Web-Services. Analysis, Assessment and Planning* / D. Menaske, V. Almeyda. – SPb: «DiaSoftJUP» Ltd., 2003. – 408 p.
3. Looker N. *Dependability Assessment of Grid Middleware, dsn* / N. Looker, J Xu // 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), 2007. – P. 125-130.
4. Looker N. *Assessing the Dependability of OGSA Middleware by Fault Injection* / N. Looker // Symposium on Reliable Distributed Systems, 2003. – P. 293-302.
5. Kalavathy G. Maria. *Parallel Performance Monitoring Service for Dynamically Composed Media Web Services* / G. Maria Kalavathy, P. Seethalakshmi // Journal of Computer Science 2009. – Vol. 5 (7). – P. 487-492.
6. McGregor C. *A framework for analyzing and measuring business performance with web services* / C. McGregor, J. Schiefer // Proceedings of the IEEE International Conference on E-Commerce, June 24-27, IEEE Xplore Press, USA, 2003. – P. 405-412.
7. Tartanoglu F. *Coordinated Forward Error Recovery for Composite Web Services* / F. Tartanoglu, V. Issarny, A. Romanovsky, N. Levy // The 22 Symposium on Reliable Distributed Systems, Italy, 2003 – P. 167-176.
8. Kharchenko V. *On Dependability of Composite Web Services with Components Upgraded Online* / V. Kharchenko, P. Popov, A. Romanovsky // Proceedings of the International Conference on Dependable Systems and Networks, Italy, 2004. – P. 287-291.

Поступила в редколлегию 1.04.2010

**Рецензент:** д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.

### ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ОЦІНКИ ГАРАНТОЗДАТНОСТІ WEB-СЕРВІСІВ

А.В. Боярчук, О.О. Гордєєв, С.М. Братушка, Р.М. Головань

*Визначена концепція інформаційної технології оцінки гарантоздатності Web-сервісів. Проведений аналіз наявних інструментальних засобів пошуку вразливостей Web-сервісів. Зроблений опис модулів профілювання, додавання несправностей, забезпечення гарантоздатності Web-сервісів. Сформований перелік несправностей та їх опис.*

**Ключові слова:** Web-сервіс, несправність, профілювання, сканери вразливостей.

### INFORMATIONAL TECHNOLOGY FOR ASSESSMENT OF WEB-SERVICES DEPENDABILITY

A.V. Boyarchuk, A.A. Gordeyev, S.N. Bratushka, R.N. Golovan

*The concept of information technology for assessment of dependability Web-services is defined. The analysis of existing instrumental tools for searching of vulnerabilities in Web-services is carried out. The modules for profiling, injecting vulnerability, ensuring dependability are developed. The set of faults and their description are proposed.*

**Keywords:** Web-service, faults, profiling, vulnerability scanner.