УДК 004.05, 004.42

О.О. ЛЕТИЧЕВСЬКИЙ
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *oleksandr.letychevskyi@litsoft.com.ua.*

В.С. ПЕСЧАНЕНКО
Херсонський державний університет, Херсон, Україна,
e-mail: *volodymyr.peschanenko@litsoft.com.ua.*

Я.В. ГРИНЮК
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *yaroslav.hryniuk@gmail.com*.

ТЕХНІКА НЕЧІТКОГО ТЕСТУВАННЯ ТА ЇЇ ВИКОРИСТАННЯ В ЗАДАЧАХ КІБЕРБЕЗПЕКИ

Анотація. Розглянуто технологію нечіткого тестування, яка полягає у тестуванні програмних систем з поданням критичних або неочікуваних вхідних даних. Наведено огляд поточного стану проблеми та представлено основні системи нечіткого тестування. Проаналізовано підхід до технології нечіткого тестування з використанням алгебричних методів, зокрема символьного моделювання. Розглянуто алгоритм «легкої ваги», який розроблено для скорочення часу генерації тестів. Алгоритм реалізовано в середовищі системи інсерційного моделювання та апробовано в тестуванні давно відомих версій систем, розроблених в ОС Linux.

Ключові слова: нечітке тестування, вразливості в програмному забезпеченні, символьне моделювання, алгебра поведінок, інсерційні моделі.

ВСТУП

Термін «нечітке тестування» є українським аналогом терміну «fuzzing» або «fuzz testing», що активно використовується в останні десять років у процесі розроблення програмного та апаратного забезпечення. Нечітке тестування на відміну від традиційних видів полягає у створенні тестів, які без визначення цілі тестування можуть викликати збій в програмному або апаратному забезпеченні.

Якщо в традиційному тестуванні ціллю тесту є перевірка функціональності системи та відповідність між реальною поведінкою та очікуваними результатами роботи системи із заданими вхідними даними, то в техніці нечіткого тестування як вхідні дані розглядають критичні або неочікувані дані, що можуть призвести до падіння системи або її непередбаченої роботи. Подання на вхід некоректних даних — це метод визначення стійкості системи до шкідливого втручання зловмисників або захищеності від збоїв зовнішніх систем, з якими вона інтегрована.

Впродовж останніх двох десятиліть створено клас систем, що реалізує техніку нечіткого тестування, а саме системи fuzzers. Ці системи розроблялись як для тестування, так і для визначення вразливостей коду. Великих успіхів досягнуто у виявленні вразливостей нульового дня, тобто таких, які ще невідомі користувачам чи розробникам програмного забезпечення. Об'єктом нечіткого тестування може бути як окремий виконуваний файл, так і операційна система, керувальний пристрій, мережевий маршрутизатор, мобільний телефон, медичний пристрій тощо.

ОГЛЯД СУЧАСНИХ СИТЕМ НЕЧІТКОГО ТЕСТУВАННЯ

Система нечіткого тестування зазвичай містить такі складові.

— Компонента створення тестових наборів, що являє собою інтелектуальну систему, яка зможе згенерувати тестові випадки, що викликають збій або непередбачену поведінку в програмному або апаратному забезпеченні.