РЕЦЕНЗІЯ

рецензента, д.т.н., професора Кучук Н.Г.

на дисертаційну роботу **Цао Вейлінь**

«МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ»,

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

1. Актуальність теми та зв'язок з науковими планами і програмами

Тема дисертаційної роботи Цао Вейлінь «Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення» є дуже актуальною в сучасному світі, оскільки все більше і більше компаній, організацій та установ залежать від програмного забезпечення для роботи та забезпечення безпеки даних та інформації. За цієї ситуації, дедалі більша увага приділяється питанням забезпечення якості та безпеки програмного забезпечення.

Технології тестування на проникнення є ефективним способом виявлення потенційних уразливостей та порушень безпеки програмного забезпечення. Ці технології дозволяють здійснювати імітацію різних видів атак на програмне забезпечення, щоб виявити можливі проблеми та недоліки у системі захисту. Застосування технологій тестування на проникнення дозволяє виявляти помилки та проблеми безпеки в програмному забезпеченні на ранніх етапах розробки, коли виправлення помилок ще не є дорогим та часом затратним процесом.

Враховуючи вищевикладене, можна вважати, що тема дисертаційної роботи Цао Вейлінь, яка спрямована на вирішення задачі розробки методу підвищення безпеки програмного забезпечення (ПЗ) з урахуванням можливостей синтезу технологій автоматизованого тестування безпеки ПЗ та глибокого машинного навчання, є актуальною з наукової та практичної точок зору, має важливу наукову та технічну значущість.

2. Зв'язок роботи з науковими програмами, планами, темами

Дисертація виконувалась відповідно до наукової програми 123 – Комп'ютерна інженерія, яка була впроваджена на кафедрі комп'ютерної інженерії НТУ «ХПІ».

3. Аналіз змісту дисертації. Ступінь обгрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

Робота Цао Вейлінь є завершеною науковою роботою, містить дві анотації – українською та англійською мовами, вступ, чотири розділи, висновки, список літератури і додаток.

Дисертація присвячена вирішенню актуальної науково-технічної задачі розробки методу підвищення безпеки програмного забезпечення (ПЗ) з урахуванням можливостей синтезу технологій автоматизованого тестування безпеки ПЗ та глибокого машинного навчання.

Об'єкт дослідження. Процес безпеки програмного забезпечення.

Предмет дослідження. Метод підвищення безпеки програмного забезпечення.

Методи дослідження. Дослідження життєвого циклу програмного забезпечення та процесів тестування, що супроводжують цей цикл, було виконано за допомогою теорії графів (GERT-моделювання). Розробку та дослідження методу автоматизованого тестування безпеки проводили методом глибокого навчання з підкріпленням. Удосконалення методики оцінки ефективності розробленої методики здійснювалось за допомогою методу динаміки середніх величин. Оцінку достовірності теоретичних і практичних результатів проводили з використанням положень теорії ймовірностей і математичної статистики.

В роботі проведено аналіз уразливостей ПЗ, зазначено на пріоритетність вимог безпеки ПЗ та обов'язковість дотримання цих вимог на всіх етапах життєвого циклу ПЗ. Проведено дослідження та порівняльний аналіз методик виявлення вразливостей, вказано на недостатність уваги з боку розробників питань безпеки. Проаналізовано основні напрямки та підходи математичного

моделювання, виділено перспективні напрямки математичної формалізації процесів тестування безпеки програмного забезпечення.

Розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи, що відрізняється від відомих врахуванням можливостей тестування безпеки спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність влучення часу виконання алгоритму тестування на проникнення в заданий інтервал.

Розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи набула подальшого розвитку (модифікована). Відмінною особливістю даної моделі є використання розподілу Ерланга як основного при математичній формалізації процесів переходу зі стану.

Розроблено метод автоматичного тестування на проникнення. Відмінною особливістю методу є комплексне використання пошукової системи Shodan, платформи аналізу мережевої безпеки MulVal, а також даних про вразливість програмного забезпечення – CVE для отримання вхідних даних та побудови реалістичних сценаріїв атак та перевірки у рамках технології глибокого навчання із підкріпленням.

При дослідженні, відповідно до методу глибокого навчання з підкріпленням, були використані оцінки винагороди, що призначаються кожному вузлу відповідно до рейтингу CVSS. Це дозволило зменшити дерева атак та визначити атаку з більшою ймовірністю виникнення.

Для оцінки застосовності методу проведено експеримент та згенеровано дерево атак, також сформовано сценарій тестування та навчання. Підтверджено факт, що навіть за невеликої кількості сценаріїв навчання результати моделювання досягають значення 0.9 щодо найбільш раціонального шляху атаки.

Вдосконалено спосіб оцінки ефективності методу тестування безпеки ПЗ. Його відмінністю є врахування можливості масштабування процесу розробки ПЗ

шляхом впровадження фахівців з тестування безпеки (DevSecOps, SecDev, а також тестувальників на проникнення).

За допомогою вдосконаленого способу доведено доцільність використання розробленого методу підвищення безпеки ПЗ з урахуванням можливостей технології глибокого навчання з підкріпленням.

Висновки, сформульовані у роботі, висвітлюють результати дослідження як вирішення висунутих в дисертації завдань. В цілому висновки відповідають вимогам, які висуваються до результатів дисертаційного дослідження на здобуття наукового ступеня доктора філософії.

Додаток містить інформацію про практичне впровадження результатів дисертації.

4. Наукова новизна одержаних результатів

Дисертація містить наукову новизну, з найбільш суттєвих доробок роботи можна назвати:

1. Вперше був розроблений метод автоматизованого тестування на вторгнення з використанням пошукової системи Shodan, платформи аналізу безпеки мережі MulVal і даних про вразливості програмного забезпечення CVE для введення та створення реалістичних сценаріїв атак і перевірки для глибокого навчання з технологією підкріплення. Це дозволило сформувати дерево атак для різних процедур навчання, оптимізувати відповідні сценарії автоматичного тестування безпеки програмного забезпечення, а отже, підвищити ефективність процесу безпеки програмного забезпечення.

2. Удосконалено математичну модель процесу тестування на проникнення в комп'ютерні системи, відмінна від відомих можливістю тестування безпеки спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність часу тестування на проникнення в заданому інтервалі.

3. Розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи. Відмінною рисою цієї моделі є використання розподілу Ерланга як основного при математичній формалізації процесів переходу від

стану до стану. Це дозволило, з одного боку, уніфікувати математичну модель і представити процес тестування на більш високому рівні ієрархії тестування, з іншого боку, спростити його.

5. Достовірність отриманих результатів та висновків

Достовірність отриманих результатів зумовлено поставленими метою та завданнями, а також використанням відповідної методології дослідження. Крім того, достовірність заявлених положень обґрунтовується комплексним підходом у вивченні визначеного об'єкта, що також зумовлює і низку певних методів, які були використані в процесі дослідження.

6. Практична цінність одержаних результатів та рекомендації щодо їх подальшого використання

Практичне значення отриманих результатів полягає в наступному.

1. Набір математичних моделей процесу тестування на проникнення в комп'ютерних системах з використанням підходу мережевого моделювання GERT спростив схему тестування на проникнення в 1,7 рази з урахуванням можливих змін у процедурах (включаючи додавання нових процедур і сервісів) для оцінки ймовірнісно-часових характеристик та можливості її масштабування при збільшенні обсягу та складності задач, що розв'язуються.

2. Синтез основних компонентів методу автоматичного тестування на проникнення дозволив підвищити ефективність процесу забезпечення безпеки ПЗ (зменшити відносний збиток на всіх етапах життєвого циклу ПЗ у 6 разів).

Результати дисертації впроваджені та використані в діяльності компанії «Line Up», ННЦ «Інститут судових експертиз», а також використовуються в навчальному процесі НТУУ ун-т «Харківський політехнічний інститут».

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладення наукових положень та результатів в опублікованих працях

Дисертація виконана з дотримання вимог академічної доброчесності, отримані результати дають підстави говорити про оригінальність роботи. У

тексті містяться авторські ідеї, і не виявлено використання ідей інших науковців без посилання на їх роботи.

Основні положення дисертації опубліковано у 15 наукових працях, серед яких: 8 наукових статей (з них 2 включено до бази даних Scopus; 6 – у вітчизняних фахових наукових виданнях), а також 7 тез доповідей (з них 1 – включено до бази даних Scopus).

8. Недоліки та зауваження до дисертаційної роботи

1. Слід зауважити, що одним з недоліків методу тестування на проникнення є те, що він не забезпечує повну гарантію безпеки програмного забезпечення. Це означає, що програмне забезпечення може бути зібрано та розгорнуто з уразливостями, які не були виявлені під час тестування на проникнення. Крім того, тестування на проникнення може бути часово та витратно затратним процесом, особливо для великих та складних систем.

2. Ще недоліком є неповне використання технологій тестування на проникнення, яке може призвести до пропуску деяких потенційних проблем безпеки. Наприклад, якщо тестування проводиться тільки на деяких етапах розробки програмного забезпечення, а не на кожному етапі, то можуть бути пропущені деякі проблеми безпеки. Крім того, тестування на проникнення може бути не ефективним в тих випадках, коли програмне забезпечення містить відомі уразливості, які вже були використані в атаках в минулому, тому важливо забезпечити постійне моніторинг та оновлення програмного забезпечення для виявлення та запобігання новим атакам.

3. В разробленому методі існує залежність ефективності системи від якості даних, на яких вона навчалася. Якщо дані містять помилки або недостатньо представлені певні типи загроз, то це може вплинути на точність та ефективність системи. Тому важливо забезпечити якість та репрезентативність даних, на яких буде навчатися система.

4. Недоліком є складність в обробці великих обсягів даних, які виникають під час тестування та машинного навчання. Це може вимагати

використання високопродуктивних систем, що може збільшити вартість та складність розробки та експлуатації.

9. Висновки

Дисертаційна робота Цао Вейлінь «Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення» є завершеною науково-дослідною роботою, яка містить науково-обгрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тема дослідження відповідає галузі знань 12 – «Інформаційні технології» та спеціальності 123 – «Комп'ютерна інженерія».

Отже, враховуючи актуальність теми, отримані результати та певну практичну значущість вважаю, що дисертаційна робота Цао Вейлінь «Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення» відповідає вимогам 6, 7, 8, 9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціальної вченої ради Закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» від 12.01.2022 р. № 44 та вимогам до оформлення дисертації МОН України від 12.01.2017 № 40, а сам автор, Цао Вейлінь, заслуговує присудження йому наукового ступеня доктора філософії зі спеціальності 123 – «Комп'ютерна інженерія».

Рецензент –доктор технічних наук,
професор кафедри комп'ютерної
інженерії та програмування Національного
Технічного Університету «Харківський
Політехнічний Інститут» Ніна КУЧУК

Підпис Н.Т.К. Ніна Кучук
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
_____
"___" _____ р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет "Харківський політехнічний інститут"
код 02071180
ЗАЙЦЕВ Ю. І.