РЕЦЕНЗІЯ

рецензента, Гавриленко Світлани Юріївни.

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

Однією з вимог, що пред'являється до сучасних комп'ютерних систем, є покращення якості та безпеки програмного забезпечення, а також забезпечення конфіденційності та стійкості до кібератак. У методології розробки програмного забезпечення відома історична роль відведена діяльності, що забезпечує відповідну його якість - тестуванню.

Основним результатом, такої діяльності, є забезпечення вимог щодо програмного забезпечення, у тому числі вимог до його безпеки. Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення, дозволить покращити основні ймовірністно-часові характеристики процесу проектування та використання програмного забезпечення, що в свою чергу підвищить ефективність розробки та впровадження програмного забезпечення на практиці.

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 глибинного машинного навчання, є актуальною з наукової та практичної точок зору, має важливу наукову та технічну цінність.

Особливу увагу автор приділив вирішенню наступних задач:

1. Аналіз основних вимог до якості програмного забезпечення, аналіз та порівняльні дослідження методів тестування програмного забезпечення на

проникнення, обґрунтування вибору напрямку дослідження та формалізація постановки наукової проблеми.

2. Розробка комплексу математичних моделей процесу тестування на проникнення в комп'ютерні системи з використанням підходу GERT-мережевого моделювання.

3. Побудова математичної моделі процесу тестування на проникнення в комп'ютерні системи з урахуванням можливостей тестування захищеності спеціалізованих інформаційних платформ комп'ютерних систем.

4. Побудова математичної моделі процесу тестування на проникнення в комп'ютерні системи, використовуючи розподіл Ерланга в якості основного при математичній формалізації процесів переходу від стану до стану

5. Розробка методу автоматичного тестування на вторгнення з урахуванням можливостей пошукової системи Shodan, платформи аналізу безпеки мережі MulVal і бази даних CVE, що містить загальновідомі вразливості інформаційної безпеки для отримання вхідних даних і побудови реалістичних сценаріїв атак з використанням технологій глибинного навчання з підкріпленням.

6. Створення методики оцінки ефективності розробленого методу підвищення безпеки програмного забезпечення.

7. Обґрунтування практичних рекомендацій щодо застосування методу підвищення безпеки програмного забезпечення.

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 обґрунтованості 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 глибинного машинного навчання.

Об'єкт дослідження. Процес безпеки програмного забезпечення.

Предмет дослідження. Методи та засоби 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 проведена методом глибинного 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 вразливостей ПЗ, зазначено пріоритетність вимог безпеки ПЗ та обов'язковість дотримання цих вимог на всіх етапах життєвого циклу ПЗ. Проведено дослідження та порівняльний аналіз методики 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. Вказано на доцільність удосконалення існуючих методів тестування на проникнення шляхом синтезу нового методу тестування з урахуванням підвищених вимог безпеки.

В другому розділі 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 приналежності часу виконання алгоритму тестування на проникнення до заданого інтервалу.

Запропонована математична модель процесу тестування на проникнення в

комп'ютерні системи набула подальшого розвитку (модифікована). Відмінною особливістю даної моделі є використання розподілу Ерланга при математичній формалізації процесів переходу зі стану. Це дозволило з одного боку уніфікувати математичну модель і представити процес тестування на більш високому рівні ієрархії тестування, з іншого боку спростити її у 1,7 разу.

Розроблено метод автоматичного тестування на проникнення. Відмінною особливістю методу є комплексне використання пошукової системи Shodan, платформи аналізу мережевої безпеки MulVal, а також бази даних CVE, що містить дані про вразливість програмного забезпечення для отримання вхідних даних та побудови реалістичних сценаріїв атак з використанням технологій глибинного навчання з підкріпленням.

Це дозволило згенерувати дерево атак для різних процедур навчання та провести оптимізацію відповідних сценаріїв автоматичного тестування безпеки програмного забезпечення.

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

Для оцінки застосовності методу проведено експеримент та згенеровано дерево атак, 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 фахівців з тестування на проникнення) ПЗ.

В основу вдосконаленого способу оцінки ефективності методу підвищення безпеки програмного забезпечення покладено метод динаміки середніх.

За допомогою вдосконаленого способу доведено доцільність використання

розробленого методу підвищення безпеки ПЗ з урахуванням можливостей технології глибинного навчання з підкріпленням. Це дозволило знизити показник відносних збитків на всіх етапах життєвого циклу до 6 разів, залежно від можливої тривалості кібервторгнення.

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.

3. 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 на основі глибинного навчання з підкріпленням. 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. Удосконалена математична модель процесу тестування на проникнення в комп'ютерні системи, яка відрізняється 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.

4. 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 обґрунтовує використання певних методів, дослідження.

5. 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 до 6 разів).

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

6. 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 проіндексовані в наукометричній базі Scopus; 6 – у вітчизняних фахових наукових виданнях), а також 7 тез доповідей (з них 1 – проіндексована в наукометричній базі Scopus).

7. Недоліки та зауваження до дисертаційної роботи

1. Слід зауважити, що постановочна частина дисертації виглядала б краще, якби більшої уваги було надано порівняльному аналізу існуючих математичних методів та платформ тестування програмного забезпечення. Це підвищило б ступінь обґрунтованості зроблених автором висновків, щодо необхідності удосконалення існуючих та розробки нових підходів щодо використання методів тестування на проникнення.

2. На рис. 3.6. запропонована топологічна структура досліджуваної комп'ютерної мережі з вже застарілим програмним забезпеченням. На сьогодні, в таких схемах існує можливість використання більш сучасного програмного забезпечення з додатковими елементами захисту даних.

3. В четвертому розділі автор пропонує занадто спрощену структурну схему методу оцінки ефективності розробленого методу підвищення безпеки програмного забезпечення. Наявність такої малої кількості учасників процесу на схемі знижує практичну значущість методу оцінки ефективності.

4. В четвертому розділі надаються практичні рекомендації щодо використання розробленого методу. Нажаль в цих практичних рекомендаціях не вказано перспективи застосування методів моделювання (GERT-моделювання та моделювання за допомогою технологій глибинного навчання).

8. Висновки

Дисертаційна робота Цао Вейлінь «Метод підвищення безпеки програмного забезпечення на основі технологій тестування на проникнення» є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та дає перспективи подальших досліджень. Тема дослідження

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».

Перший рецензент, професор кафедри комп'ютерної інженерії та програмування НТУ «ХПІ», доктор технічних наук, професор — Світлана ГАВРИЛЕНКО

Посада, науковий ступінь, вчене звання *підпис* *ПІБ*

12 червня 2023 р

Підпис проф. Світлани Гавриленко
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
"___" _____ 20____ р.

ЗАПІЦЕВ К. А.