РЕЦЕНЗІЯ

рецензента, Гавриленко Світлани Юріївни.

на дисертаційну роботу **Чжан Ліцзян**

«Метод підтримки прийнятих рішень щодо безпеки програмного забезпечення»

подану на здобуття наукового ступеня доктора філософії

за спеціальністю 123 – Комп'ютерна інженерія

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

Дисертаційна робота Чжан Ліцзян присвячена розробці нових методів підтримки прийнятих рішень щодо безпеки програмного забезпечення, через підвищену увагу питанням безпеки програмного забезпечення. Необхідність розробки цих методів обумовлена все більшим використанням засобів комп'ютерної техніки у всіх сферах життєдіяльності суспільства, зокрема у системах критичного застосування або системах, що використовують технології BigData. Це призводить до необхідності пришвидшення темпів розробки програмного забезпечення, що викликає іноді нехтування питаннями безпечного програмування та тестування безпеки. В умовах використання гнучких методологій розробки програмного забезпечення існують можливості адаптивного застосування ресурсів фірм-розробників програмних засобів. Але, на жаль, існуючий стан технологій та методів тестування безпеки програмного забезпечення показує здебільше нехтування питаннями використання систем підтримки прийняття рішень. Викликане це, з одного боку, нестачею фахівців та небажанням фірм нести додаткові витрати, з іншого боку, відсутністю моделей та методів тестування, що могли підвищити ефективність цього процесу.

Використання розроблених моделей та методів дозволить організаціям-виробникам програмного забезпечення скорегувати плани тестування безпеки програмного забезпечення, та більш ефективно використовувати існуючий потенціал фірм з врахуванням підвищених вимог щодо захисту інформації.

Таким чином, розроблення методів підтримки прийнятих рішень щодо безпеки програмного забезпечення є актуальним науковим завданням.

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

Дисертація виконувалась відповідно до наукової програми 123 – Ком'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 Чжан Ліцзян 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 підтримки прийняття рішень щодо безпеки програмного забезпечення (ПЗ) з урахуванням факторів невизначеності вхідних та проміжних даних тестування.

Об'єктом дослідження є процес безпеки програмного забезпечення.

В роботі проведено аналіз основних методів виявлення вразливостей програмного забезпечення. Показано, що використання існуючих методів та технологій аналізу безпеки не забезпечує точності результату, особливо в умовах нечітких вхідних даних.

За результатами дослідження запропоновано математичну модель процесу підготовки до тестування безпеки, яка відрізняється від відомих теоретично обґрунтованим вибором генеруючих функцій моментів при опису переходів зі стану в стан, наявністю етапу перевірки вихідного коду на криптографічні та інші методи захисту даних, що дозволило отримати аналітичні вирази для розрахунку імовірнісних характеристик та використати їх подалі в загальному процесі тестування програмного забезпечення.

Розроблено GERT-мережу процесу підготовки до тестування безпеки, GERT-мережу процесу перевірки вихідного коду на предмет наявності криптографічних та інших способів захисту даних та GERT-модель першого етапу тестування програмного забезпечення на безпеку. У сукупності розроблено математичну модель процесу підготовки до тестування безпеки, яка відрізняється від відомих, теоретично обґрунтованим вибором генеруючих функцій моментів, при описі переходів із стану в стан, а також наявністю етапу перевірки вихідного коду на предмет криптографічних та інших способів захисту даних.

Розроблено чітку GERT-мережу для процесу дослідження вразливості програмного забезпечення та виявлено її недоліки, які пов'язані з неврахуванням нечіткості вхідних даних і перехідних характеристик і процесів.

На основі математичного апарату нечіткого мережевого моделювання вперше розроблено нечітку GERT-модель дослідження вразливостей програмного забезпечення. Відмінною особливістю даної моделі є урахування ймовірнісних характеристик переходів із стану в стан у сукупності з поточними характеристиками. В рамках моделювання виконано наступні етапи дослідження. Для схематичного опису процедури дослідження вразливостей програмного забезпечення розроблено структурну модель цього процесу. Визначено «еталонну GERT-модель» дослідження вразливостей програмного забезпечення. При цьому, цей процес був описаний у вигляді стандартної GERT-мережі. Удосконалено алгоритм еквівалентних перетворень GERT-мережі, що відрізняється від відомих урахуванням можливостей розширеного спектру типових структур паралельних гілок сусідніх вузлів. Представлено аналітичні результати для розрахунку середнього часу перебування у гілках і ймовірності

успішного завершення дослідження в кожному вузлу. Проведено розрахунок вказаних ймовірнісно-часових характеристик відповідно до даних уточненої еквівалентної нечіткої GERT-мережі процесу дослідження вразливостей програмного забезпечення. Проведені порівняльні дослідження для підтвердження достовірності отриманих результатів. Результати експерименту показали співмірність ймовірнісних і часових показників, отриманих за допомогою вдосконаленого алгоритму еквівалентного перетворення зі значеннями, отриманими в результаті реалізації відомих еталонних алгоритмів.

За результатами дослідження розроблено метод підтримки прийняття рішення про безпеку програмного забезпечення. Відмінною особливістю методу є використання удосконаленого методу генерації навчальної вибірки, яка включає три рівні генерації: генерація навчальної вибірки, генерація навчального прикладу та генерація конкретного значення характеристики безпеки. Це дозволило підвищити точність класифікації та прийняття рішень

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.

Список літератури досить широко охоплює предметне поле дослідження, певною мірою відображає опрацювання автором значної кількості джерел.

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 розроблено нечітку модель GERT для дослідження вразливостей програмного забезпечення. Відмінною особливістю даної моделі є те, що вона

враховує поряд з часовими характеристиками ймовірнісні характеристики переходів із стану в стан. Це дозволило зменшити нечіткість вихідних характеристик часу проведення досліджень вразливостей програмного забезпечення та підвищити точність моделювання.

2. Удосконалено математичну модель процесу підготовки до перевірки безпеки, яка відрізняється від відомих теоретично обґрунтованим вибором генеруючих функцій моментів при описі переходів від стану до стану, а також врахуванням етапу перевірка вихідного коду на наявність криптографічних та інших методів захисту інформації, що дало змогу отримати аналітичні вирази для розрахунку імовірнісних характеристик та використати їх в подальших розрахунках.

3. Подальший розвиток отримав метод підтримки прийняття рішень щодо безпеки програмного забезпечення. Відмінною особливістю методу є синтез удосконаленого методу генерації навчальної вибірки в процесі навчання штучної нейронної мережі. Це дало змогу підвищити ефективність методу та підвищити точність класифікації та прийняття рішень щодо безпеки програмного забезпечення.

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 обґрунтовує використання певних методів, дослідження.

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

Практичне значення отриманих результатів полягає у підвищенні точності

прийняття рішень щодо безпеки програмного забезпечення, за рахунок використання апарату нечіткого моделювання та нечітких множин.

Практичне значення отриманих результатів полягає в наступному.

1. Використання нечіткої моделі GERT у процесі дослідження вразливостей програмного забезпечення підвищило точність моделювання до 13%.

2. Використання вдосконаленого алгоритму спрощення еквівалентних перетворень у моделюванні дозволило зменшити нечіткість вихідних характеристик часу проведення досліджень вразливостей програмного забезпечення до 1,12 рази.

3. Впровадження методики навчання штучної нейронної мережі в метод підтримки прийняття рішень щодо безпеки програмного забезпечення дозволило підвищити ефективність оцінки безпеки програмного забезпечення до 1,2 разів.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження.

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

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

Надану здобувачем дисертацію виконано відповідно Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 № 40 та із змінами, внесеними згідно з Наказом Міністерства освіти і науки № 759 від 31.05.2019.

Порушень академічної доброчесності (академічного плагіату, самоплагіату, фабрикації, фальсифікації) в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації не виявлено, про що свідчить аналіз звітів перевірки дисертації на наявність плагіату.

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 – проіндексовані в наукометричній базі Scopus).

8. Недоліки та зауваження до дисертаційної роботи

1. У другому розділі дисертаційної роботи не вказано обмеження використання математичного апарату GERT-мереж. Врахування обмежень дозволило б підвищити практичну значущість розробки.

2. У третьому розділі не достатньо обґрунтовано використання трапецієподібних нечітких чисел при оцінці часу дослідження вразливостей програмного забезпечення.

3. Для підтвердження ефективності автор виконав порівняльний аналіз лише з моделями на основі алгоритмів Гаварешки и Хашимина. Виконання порівняльного аналізу з більшою кількістю алгоритмів та моделей було б більш доцільним.

4. У четвертому розділі автор удосконалює метод навчання штучної нейронної мережі, що відрізняється способом генерації вибірки, що навчається. Нажаль, функції генерації вибірки автор не наводить.

5. У четвертому розділі доцільно було б оцінити якість класифікації методу підтримки прийняття рішень щодо безпеки програмного забезпечення іншими показниками якості, наприклад, Precision, Recall, F1-score. Це дозволило б дослідити оптимальний поріг прийняття рішення (Threshold) та знайти баланс між чутливістю та специфічністю моделі.

9. Висновки

Дисертаційна робота Чжан Ліцзян є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані результати, має наукову новизну та має перспективи для 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 Чжан Ліцзян «Метод підтримки прийнятих рішень щодо безпеки програмного забезпечення» 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, Чжан Ліцзян, заслуговує присудження їй 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. Світлана Гавриленко
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ЗАЙЦЕВ Ю. І.
"___" _____ 20___ р.