РЕЦЕНЗІЯ

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

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

Зростаюча кількість кібератак та кіберзлочинів, що стаються в світі, роблять безпеку програмного забезпечення більш актуальною темою, ніж будь-коли раніше. Захист від кібератак стає надзвичайно важливим для багатьох компаній, установ та громадян, які користуються комп'ютерами та мережами. Компанії та організації, які працюють з конфіденційними даними, повинні бути особливо уважні до захисту своїх систем та даних.

Метод підтримки прийнятих рішень щодо безпеки програмного забезпечення може допомогти компаніям та організаціям виявити та усунути потенційні проблеми безпеки ще до того, як вони стануть проблемами реального рівня. Це може допомогти компаніям та організаціям зменшити ризики та втрати, пов'язані з кібератаками та іншими безпековими проблемами.

Дисертаційна робота Чжан Ліцзян присвячена розробці нових методів підтримки прийнятих рішень щодо безпеки програмного забезпечення, через підвищену увагу питанням безпеки програмного забезпечення.

Отже, метод підтримки прийнятих рішень щодо безпеки програмного забезпечення залишається важливою темою для компаній, організацій та громадян, які хочуть захистити свої системи та даними від кіберзагроз а вирішення проблеми, що зазначена в дисертаційній роботі є актуальним науковим завданням.

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 та програмування НТУ «ХПІ».

3. Аналіз змісту дисертації. Ступінь обгрунтованості 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.

Розроблено модель GERT для першого етапу тестування безпеки програмного забезпечення. Модель відрізняється від відомих теоретично обґрунтованим вибором моментоутворюючих функцій при описі переходів від стану до стану, а також врахуванням початкової фази перевірки коду для методів криптографічного захисту.

Розроблено структурну модель проведення досліджень уразливостей програмного забезпечення. На її основі розроблено чітку GERT-мережу процесу досліджень вразливостей програмного забезпечення. Виявлено недоліки цієї мережі, пов'язані з зневагою нечіткості вхідних даних та перехідних характеристик та процесів.

На основі математичного апарату нечіткого мережевого моделювання вперше розроблено нечітку GERT-модель дослідження вразливостей програмного забезпечення. Відмінною особливістю даної моделі є врахування

імовірнісних характеристик переходів зі стану до стану поряд з часовими характеристиками. Проведено порівняльні дослідження для підтвердження достовірності одержаних результатів.

Розроблено метод підтримки ухвалення рішення про безпеку ПЗ. Відмінною особливістю методу є синтез удосконаленого способу генерації навчальної вибірки процес навчання штучної нейронної мережі.

Удосконалено метод навчання штучної нейронної мережі, що відрізняється способом генерації вибірки, що навчається. Даний спосіб генерації включив три рівні генерації: генерація навчальної вибірки, генерація навчального прикладу і генерація конкретного значення характеристики безпеки.

З використанням процедур ROC-аналізу проведено дослідження ефективності методу підтримки прийняття рішення про безпеку ПЗ. Результати експерименту підтвердили гіпотезу про ефективність розробленого методу підтримки прийняття рішення про безпеку ПЗ до 1,2 разів у порівнянні з методами, в основі яких використовуються положення дискримінантного та кластерного аналізу.

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.

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 твірних 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 математичними методами отримати аналітичні вирази для розрахунку імовірнісних характеристик для дослідження та більш складних комп'ютерних систем.

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 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 у підвищенні точності прийняття рішень щодо безпеки програмного забезпечення, використовуючи

технології 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 уразливостей програмного забезпечення до 1,12 рази.

3. Впровадження методу навчання штучної нейронної мережі в загальну методику підтримки прийняття рішень щодо безпеки програмного забезпечення дозволило підвищити точність класифікації та прийняття рішень у 1,6 рази для позитивних елементів у вибірці та в 1,2 рази для негативних елементів у вибірці. зразок.

4. Використання методу підтримки прийняття рішень дозволило підвищити ефективність оцінки безпеки програмного забезпечення до 1, 2 раза.

Практичне значення отриманих результатів підтверджено відповідними актами впровадження.

Результати дисертації впроваджені та використані в діяльності компанії «Line Up», ННЦ «Інститут судових експертиз», 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

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. В дисертаційні роботі не вказано про складність реалізації та впровадження методу. Розробка та впровадження такого методу вимагає багато часу та зусиль. Крім того, для реалізації такого методу необхідно мати високий рівень знань та досвіду у сфері кібербезпеки, програмування та аналітики даних.

2. В роботі не проведено вартісна оцінка впровадження методу. Висока вартість використання такого методу є його недоліком, оскільки його використання може вимагати спеціального обладнання та програмного забезпечення. Крім того, необхідно надати достатню кількість ресурсів для забезпечення постійної підтримки та поновлення методу підтримки прийнятих рішень щодо безпеки програмного забезпечення.

3. При практичному використанні методу може виникнути проблема зі збиранням достатньої кількості даних для аналізу та розробки алгоритмів підтримки прийнятих рішень. Недостатньо обсягу даних або недоступність даних може обмежувати можливості вдосконалення та впровадження методу.

4. Ще одним недоліком може бути те, що метод підтримки прийнятих рішень щодо безпеки програмного забезпечення може бути не ефективним в роботі з новими видами загроз, які не були враховані при розробці алгоритмів підтримки прийнятих рішень. Це може вимагати постійного вдосконалення та модифікації методу.

9. Висновки

Дисертаційна робота Чжан Ліцзян є завершеною науково-дослідною роботою, яка містить науково-обґрунтовані 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 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 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 Ніни Кучук
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ЗАЙЦЕВ Ю. І.
" " 20 р.