ВІДГУК

офіційного опонента
Трубчанінової Карини Артурівни
на дисертаційну роботу **Чжан Ліцзян**
«МЕТОД ПІДТРИМКИ ПРИЙНЯТИХ РІШЕНЬ ЩОДО БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 123 - Комп'ютерна інженерія

Актуальність теми

З кожним роком зростає кількість кібератак, які спрямовані на отримання доступу до конфіденційної інформації, викрадення грошей або пошкодження інфраструктури компанії. Також зростає кількість програмного забезпечення, яке використовуєгься в різних сферах життя, що створює нові можливості для кіберзлочинців.

Метод підтримки прийнятих рішень щодо безпеки програмного забезпечення може допомогти забезпечити ефективний захист від кібератак і запобігти можливим порушенням безпеки. Цей метод полягає у визначенні інформації про ризики, пов'язані з програмним забезпеченням, та прийнятті рішень про вжиття заходів щодо зменшення цих ризиків.

Окрім того, забезпечення безпеки програмного забезпечення є важливим елементом в розвитку технологій та інформаційного суспільства. Це допомагає підтримувати довіру користувачів до програмного забезпечення та стимулювати розвиток інновацій в галузі інформаційних технологій.

Все вищезазначене свідчить про актуальність науково-технічної задачі, що складається в підвищенні точності прийняття рішень щодо безпеки програмного забезпечення на основі синтезу комплексу математичних моделей і методу підтримки прийняття рішень щодо безпеки програмного забезпечення.

Отже, можна стверджувати, що гема "Метод підтримки прийнятих рішень щодо безпеки програмного забезпечення" є дуже актуальною у сучасному світі і має велике значення для забезпечення безпеки інформації та розвитку технологій.

Дисертаційну роботу виконано на кафедрі комп'ютерної інженерії Національного технічного університету "Харківський політехнічний інститут".

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Положення та висновки, наведені в дисертаційній роботі Чжан Ліцзян, в достатній мірі обґрунтовані як з наукового, так і з технічного поглядів. Обґрунтованість отриманих у роботі наукових положень, висновків і рекомендацій базується на використанні математичного апарату теорії імовірності та математичної статистики, теорії інформації, методів математичного та імітаційного моделювання з використанням ліцензійного програмного забезпечення.

Дослідження виконані з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірені шляхом проведення практичних експериментів, що підтверджує обґрунтованість наукових положень, висновків і рекомендацій, сформульованих в дисертаційній роботі.

Достовірність результатів досліджень.

Достовірність результатів теоретичних досліджень підтверджується результатами відповідних експериментальних досліджень.

Наукові результати застосовані під час створення імітаційних моделей з використання математичного пакету MathCad.

До основних нових наукових результатів дисертації слід віднести наступне:

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.

Значимість отриманих результатів для науки і практичного використання.

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 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 рази.

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 "ХПІ".

Повнота викладення результатів досліджень в опублікованих працях.

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).

Участь здобувана у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

Опубліковані матеріали повністю відображають зміст дисертації та відповідають вимогам пункту 8 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44.

Оцінка змісту дисертаційної роботи

Дисертаційна робота Чжан Ліцзян складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатку.

В першому розділі в роботі проведено аналіз основних методів виявлення вразливостей програмного забезпечення. Показано, що використання існуючих методів та методик аналізу безпеки не забезпечує точності результату в умовах

нечітких вхідних даних. Показано, що перспективним напрямом підвищення ефективності діяльності є зниження навантаження на експерта за рахунок удосконалення методів виявлення вразливостей та впровадження системи підтримки ухвалення рішення.

У другому розділі 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. Це може підвищити точність результатів тестування безпеки програмного забезпечення, а також використовувати результати в загальному процесі тестування програмного забезпечення.

Розроблено розширений алгоритм відповідності безпеки. Цей алгоритм відрізняється від відомих тим, що враховує параметри невизначеності при виборі моментоутворюючих функцій кожної гілки переходу від стану до стану GERT-мережі, що розробляється. Це могло б зменшити невизначеність вхідних даних на етапі розробки процесу підготовки мережі GERT до дослідження тестування безпеки програмного забезпечення.

Розроблено GERT-мережу для підготовки до процесу тестування безпеки. Його відмінною рисою є врахування перевірки вихідного коду на наявність криптографічних та інших способів захисту даних. Це може підвищити точність результатів моделювання в умовах такого типу кіберзловживань.

Розроблено GERT-мережу для перевірки вихідного коду на наявність криптографічних та інших способів захисту даних. Отримано аналітичні вирази та експериментально розраховано дані, використані в GERT-моделі процесу тестування безпеки програмного забезпечення.

Розроблено структурну модель проведення досліджень вразливостей 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.

У третьому розділі 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. Це дозволило підвищити точність моделювання до 13%.

Удосконалено алгоритм спрощення еквівалентних перетворень, який відрізняється від відомих з урахуванням можливостей розширеного спектра типових

структур паралельних гілок між сусідніми вузлами. Це дозволило знизити нечіткість вихідних характеристик часу проведення досліджень вразливостей (відхилення від середнього значення) до 1.12 рази.

На основі алгоритму удосконалено нечітку GERT-модель дослідження вразливостей ПЗ, що відрізняється від відомих відсутністю петель у мережній структурі.

Проведено порівняльні дослідження для підтвердження достовірності одержаних результатів. Результати експерименту показали сумісність ймовірнісних і часових показників, отриманих за допомогою вдосконаленого алгоритму еквівалентного перетворення зі значеннями, отриманими в результаті відомих еталонних алгоритмів Гаварешки і Хашиміна.

В четвертому розділі розроблено метод підтримки ухвалення рішення про безпеку ПЗ. Відмінною особливістю методу є синтез удосконаленого способу генерації навчальної вибірки процес навчання штучної нейронної мережі. Це дозволило підвищити ефективність методу підтримки прийняття рішення про безпеку програмного забезпечення до 1,2 разу.

У ході дослідження було розроблено модель формування векторів вхідних даних. Відповідно до даної моделі для формування вхідних даних формується множина ознак потенційних вразливостей та недекларованих можливостей ПЗ відповідно до даних PVS-Studio Analysis Results.

Як дизайн архітектури нейронної мережі для вирішення задачі підтримки прийняття рішення про безпеку ПЗ було запропоновано за основу взяти багатошаровий персептрон.

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. Це дозволило підвищити точність класифікації та прийняття рішення у 1,6 рази для позитивних елементів у вибірці та у 1,2 рази для негативних елементів у вибірці.

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 до розділів та за результатами роботи сформульовані чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел із 127 найменувань досить повний і включає

вітчизняні та зарубіжні публікації.

Анотація відображає основний зміст дисертації та достатньо повно розкриває наукові результати та практичну цінність роботи.

Академічна доброчесність

Порушень академічної доброчесності в дисертації та наукових публікаціях, у яких висвітлені основні наукові результати дисертації, не виявлено.

Усі результати, які винесено автором на захист, отримані самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

По дисертаційній роботі можна зробити наступні зауваження:

1. Нажаль робота не містить практичних прикладів застосування методу підтримки рішень щодо безпеки програмного забезпечення, що може зменшити практичну цінність роботи. Для покращення цього аспекту, можна додати приклади застосування методів підтримки рішень у реальному житті.

2. Робота містить має дуже обмежений обсяг порівняльних прикладів методу підтримки рішень з іншими методами захисту від кібератак, що може зменшити повноту та обґрунтованість роботи. Для покращення цього аспекту, можна додати порівняння з іншими методами захисту від кібератак та навести переваги та недоліки кожного з методів.

3. Підтвердження достовірності результатів моделювання автор проводить оцінкою сумісності ймовірнісних і часових показників, отриманих за допомогою вдосконаленого алгоритму еквівалентного перетворення зі значеннями, отриманими в результаті відомих еталонних алгоритмів Гаварешки і Хашиміна. Такий підхід оцінки достовірності не є раціональнім і точним. Потрібно було використовувати більш відомі методи оцінки достовірності.

4. В дисертації не зроблено акцентів, на те, яку саме інформацію та програмне забезпечення автор рекомендує захищати за допомогою розробленого методу, та які особливості захисту різного програмного забезпечення.

Вказані недоліки не впливають на загальну позитивну оцінку виконаної роботи. Дисертація є актуальною і має високу наукову цінність та практичну значущість.

ВИСНОВОК

Дисертаційна робоча Чжан Ліцзян «МЕТОД ПІДТРИМКИ ПРИЙНЯТИХ РІШЕНЬ ЩОДО БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ» за своїм змістом відповідає спеціальності 123 – Комп'ютерна інженерія. Дисертація є завершеною науково-дослідною роботою, яка розв'язує важливу науково-практичну задачу, що

складається в підвищенні точності прийняття рішень щодо безпеки програмного забезпечення на основі синтезу комплексу математичних моделей і методу підтримки прийняття рішень щодо безпеки програмного забезпечення..

Подана дисертаційна робота Чжан Ліцзян «МЕТОД ПІДТРИМКИ ПРИЙНЯТИХ РІШЕНЬ ЩОДО БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ» відповідає спеціальності 123 - Комп'ютерна інженерія, відповідає вимогам до дисертацій на здобуття наукового ступеня доктора філософії, а саме вимогам пунктів 6, 7, 8 і 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого Постановою КМУ від 12.01.2022 р. №44, а здобувач Чжан Ліцзян заслуговує присудження наукового ступеня доктора філософії за спеціальністю 123 - Комп'ютерна інженерія.

Офіційний опонент
Професор кафедри транспортного зв'язку
Українського державного університету
залізничного транспорту, д.т.н., професор
12.06.2023 Карина ТРУБЧАНІНОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Український державний університет залізничного транспорту * №01116472

Особистий підпис
засвідчую 12.06 2023 р.
Завідуючий канцелярією
УкрДУЗТ

Карина Трубчанінова
Шилко