ВІДГУК

офіційного опонента

завідувача кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки, доктора технічних наук, професора Коваленка Андрія Анатолійовича 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

Існуючі тенденції загального використання комп'ютерних та комп'ютеризованих засобів обумовлюють і високий рівень вимог щодо розроблюваного програмного забезпечення. При цьому вимоги до безпеки програмного забезпечення є ще більш високими у зв'язку із збільшенням випадків кібератак. Особливо жорсткі вимоги безпеки висуваються до програмного забезпечення комп'ютерних систем критичного застосування, де ступінь ризику є надзвичайно високою. Однак, як показують події останніх років, нехтування питаннями безпеки програмних засобів в процесі розробки призводить лише до збільшення кількості успішно проведених кібератак і, відповідно, до економічних, фінансових, іміджевих та інших втрат підприємств і держави в цілому.

Одним з основних завдань науковців в означеному напрямі є удосконалення існуючих методів тестування безпеки програмного забезпечення для захисту інформації. Таке завдання широко розглядається в сучасних наукових публікаціях. Однак відомі роботи більшою мірою мають криптографічну спрямованість і не мають на меті підвищення безпеки на етапах життєвого циклу розробки програмного забезпечення. Крім того, у більшості досліджень не враховується динаміка можливих змін та можливість використання систем підтримки прийняття рішень. 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.

Дисертаційну роботу виконано на кафедрі комп'ютерної інженерії та програмування 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 ймовірності та математичної статистики, теорії інформації, методів математичного та імітаційного моделювання з використанням ліцензійного програмного забезпечення.

Дослідження виконано з використанням математичного апарату та сучасного комп'ютерного моделювання. Результати перевірено 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 вивчення вразливостей програмного забезпечення. Відмінною особливістю цієї моделі є те, що вона враховує поряд з тимчасовими характеристиками ймовірнісні характеристики переходів зі стану. Це дозволило зменшити нечіткість вихідних характеристик часу проведення досліджень уразливостей програмного забезпечення та підвищити точність моделювання.

2. Удосконалено математичну модель процесу підготовки до тестування безпеки, яка відрізняється від відомих теоретично обґрунтованим вибором функцій, що виробляють, моментів при описі переходів зі стану в стан, а також з урахуванням етапу перевірки вихідний код криптографічних та інших методів захисту інформації, що дозволив отримати математичними методами аналітичні вирази для розрахунку ймовірнісних показників для дослідницьких і складніших обчислювальних систем.

3. Подальший розвиток отримав метод підтримки прийняття рішень щодо безпеки програмного забезпечення. Відмінною особливістю методу є синтез удосконаленого методу формування навчальної вибірки у процесі навчання штучної нейронної мережі. Це дозволило 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 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.

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

Практичне значення отриманих результатів підтверджено відповідними актами впровадження.

Результати дисертації впроваджені та використані в діяльності компанії "LineUp", Науково-дослідного центру судової експертизи з питань інтелектуальної власності Міністерства юстиції України, а також використовуються в навчальному процесі Національного технічного університету "Харківський політехнічний інститут".

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 здобувача у роботах, що опубліковані у співавторстві зазначена у дисертаційній роботі.

Опубліковані матеріали повністю відбивають 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, додатків.

У вступі обґрунтовано актуальність теми дисертації, показано її наукову і практична цінність, сформульовано мету і задачі дослідження, які необхідно вирішити для її досягнення, описано зв'язок дисертації з науковими планами та темами, приведено апробацію дисертаційної роботи і публікації.

У першому розділі автором виконано порівняльний аналіз основних методів виявлення вразливостей програмного забезпечення; показано негативний вплив використання існуючих методів та методик аналізу безпеки на точність результату в умовах нечітких вхідних даних.

У другому розділі виявлено проблему аргументованого вибору підходів моделювання на різних етапах процесу тестування безпеки програмного забезпечення і виявлення його вразливостей, що, в цілому, знижує точність отриманих результатів моделювання. Визначено два етапи процесу виявлення вразливостей програмного забезпечення. Розроблено удосконалений алгоритм перевірки відповідності за критерієм безпеки, відмінною особливістю параметрів, які є вибором законів і розподілу, описуючи окремі переходи від стану в стан для окремих гілок GERT-мереж. Розроблено GERT-мережу процесу підготовки до тестування безпеки. Розроблено GERT-мережу процесу перевірки вихідного коду на предмет криптографічних та інших способів захисту даних. Розроблено GERT-модель першого етапу тестування програмного забезпечення на безпеку. У сукупності, розроблено математичну модель процесу підготовки до тестування безпеки, що відрізняється від відомих теоретично обґрунтованим вибором виробничих функцій моментів, при описі переходів із стану в стан, а також з урахуванням етапу перевірки вихідного коду на предмет криптографічних та інших способів захисту даних.

У третьому розділі розроблено нечітку GERT-модель дослідження вразливостей програмного забезпечення. Відмінною особливістю моделі є урахування ймовірних характеристик переходів із стану (а не лише часових характеристик). В рамках моделювання виконано наступні етапи дослідження. Для схематичного опису процедури дослідження вразливостей програмного забезпечення розроблено структурну модель цього процесу. Розроблено «еталонну GERT-модель» дослідження вразливостей програмного забезпечення. При цьому процес було описано у вигляді стандартної GERT-мережі. Удосконалено алгоритм еквівалентних перетворень GERT-мережі, що відрізняється від відомих з урахуванням можливостей розширеного спектру типових структур паралельних гілок між сусідніми вузлами. Представлено аналітичні результати для розрахунку середнього часу перебування та ймовірності успішного завершення в кожному вузлі. Проведено розрахунок указаних ймовірно-часових характеристик відповідно до даних уточненої еквівалентної нечіткості GERT-мережі процесу дослідження вразливостей програмного забезпечення. Проведено порівняльні дослідження для підтвердження достовірності отриманих результатів. Результати експерименту довели співмірність ймовірних і часових показників, отриманих за допомогою вдосконаленого алгоритму еквівалентного перетворення зі значеннями, отриманими в результаті реалізації відомих алгоритмів.

У четвертому розділі розроблено метод підтримки прийняття рішення щодо безпеки програмного забезпечення. Відмінною особливістю методу є синтез удосконаленого методу генерації навчальної вибірки в процесі навчання штучної нейронної мережі.

Висновки до розділів та за результатами роботи сформульовано чітко та відповідають змісту дисертаційної роботи.

Список використаних джерел зі 127 найменувань досить повний та включає вітчизняні та зарубіжні публікації.

Анотація відбиває 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, отримано самостійно і містяться в опублікованих роботах. У роботах, опублікованих у співавторстві, використані тільки ті ідеї, положення та розрахунки, які є результатом особистих наукових пошуків.

За дисертаційною роботою можна зробити наступні зауваження:

1. Основні наукові результати ґрунтуються на використанні математичного апарату GERT-моделювання. Проте, обґрунтування вибору саме цього підходу до моделювання відсутнє. Доцільно було б навести порівняння ефективності використання такого підходу з іншими існуючими.
2. На рис. 2.1 при описі блок-схеми підготовки дослідження тестування безпеки, нажаль, автор наводить лише якісні показники, при цьому нехтує кількісними. Це ускладнює сприйняття опису проведеного експерименту та не дає можливості об'єктивної верифікації його результатів.
3. У третьому розділі, у схемі дослідження вразливостей програмного забезпечення, автор пропонує на заключному етапі використовувати автоматичне підтвердження потенційних вразливостей. Але, нажаль, розробок в цьому напрямку та результатів автор не наводить. Крім того, автор в роботі не пропонує окремих форматів подання вхідних даних для такого алгоритму.
4. На рис. 4.2 автором запропоновано модель штучної нейронної мережі. Нажаль, аргументів обрання саме такої моделі автор не надає.
5. В дисертації недостатньо обґрунтовано рішення про використання програмного забезпечення для реалізації задач, що поставлено в роботі.

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

ВИСНОВОК

Дисертаційна робота 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-технічну 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 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
доктор технічних наук, професор
завідувач кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки

Андрій КОВАЛЕНКО

"12" 06 2023 р.

ПІДПИС ЗАСВІДЧУЮ
В.о. ректора
доктор технічних наук, професор

Ігор РУБАН

"12" 06 2023 р.