ВІДГУК

офіційного опонента на дисертаційну роботу

Коваленко Олександра Володимировича

“Моделі та методи розроблення безпечного програмного забезпечення комп’ютерних систем”

на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти.

Актуальність теми дисертації.

Сучасний інформаційний простір являє собою складну, гетерогенну структуру, що виконує різноманітні функції і запити суспільства. При цьому значну частину функцій автоматизації та інтелектуалізації беруть на себе комп'ютерні системи (КС).

Шкідливі впливу на КС в цілому і програмне забезпечення зокрема, в процесі їх функціонування, здійснюються з різними зловмисними цілями порушення (погіршення) послуг безпеки. Особливо небезпечними представляються загрози безпеки програмного забезпечення.

Рішення задач, пов'язаних із запобіганням несанкціонованих впливів на програмне забезпечення здійснюється в рамках комплексних програм підвищення безпеки. При цьому проблема підвищення безпеки програмного забезпечення в повному обсязі не вирішена.

Тому дисертаційна робота Коваленко Олександра Володимировича що присвячена вирішенню наукової проблеми синтезу моделей та методів розроблення безпечного ПЗ КС є актуальною.

Дослідження в дисертаційній роботі проводилися у відповідності з наступними нормативними актами.

– Концепцією Національної Програми інформатизації, схваленої Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р. № 75\98 – ВР (зі змінами 2000 – 2012 рр.);

– Законом України «Про телекомунікації» від 18.11.2003 р. № 1280-IV.

– Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 р. № 2594-IV;

– Постановою Кабінету Міністрів України від 29.03.2006 р. №373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» (зі змінами 2006, 2011 рр.);

– планами наукової і науково-технічної діяльності Центральноукраїнського національного технічного університету, у рамках виконання науково-дослідних робіт: держбюджетних науково-дослідних робіт №36Б113 «Розробка методів підвищення оперативності передачі і захисту інформації в телекомунікаційних системах» (ДР №0113U003086), №36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі і захисту інформації в телекомунікаційних системах» (ДР №0115U003103), науково-дослідних робіт «Інформаційна технологія автоматизації проектування і тестування об'єктно-орієнтованого програмного забезпечення» (ДР №0114U003831), «Інформаційна технологія проектування тестових наборів на основі вимог до програмного забезпечення інфокомунікаційних систем» (ДР №0116U008133), в який автор є співвиконавцем окремих етапів.

Основний зміст роботи.

У вступі обґрунтовано актуальність дисертації, визначено основні наукові складові дисертаційного дослідження, мету, об’єкт та предмет дослідження. Сформульовано проблему дисертаційного дослідження, наукові завдання, наведено основні наукові та практичні результати. Відзначено особистий внесок здобувача, апробацію результатів дисертаційної роботи на конференціях, наведено відомості про публікації та структуру роботи.

У першому розділі здобувачем проведено порівняльні дослідження а також аналіз сучасних тенденцій розвитку моделей і методів розроблення безпечного програмного забезпечення. Зроблено висновки про перспективи

розвитку цих моделей і методів. Проаналізовано вимоги до програмних засобів. Проведено аналіз і порівняльне дослідження факторів, що впливають на безпеку. Наведено результати досліджень основних підходів математичного моделювання процесу розроблення безпечного програмного забезпечення. Зроблено постанову завдання дисертаційного дослідження.

У другому розділі дисертаційної роботи в ході рішення поставленої задачі на першому етапі розроблено метод якісного аналізу вразливостей розроблення програмного забезпечення.

Його відмінною особливістю є врахування факторів експлуатаційних вразливостей, особливо вразливості невиявлення загроз безпеки ПЗ і оцінкою довільного несуперечливого кінцевого набору "квантів інформації".

Однією з основних складових методу є структурна ідентифікація вразливостей розроблення ПЗ, що відрізняється від відомих побудовою оцінки вразливостей розроблення ПЗ "зверху" у вигляді множини, за наявності довільного несуперечливого кінцевого набору "квантів інформації".

На другому етапі розроблено метод кількісної оцінки вразливостей розроблення ПЗ. Його відмінною особливістю є комплексне використання "Аналізу дерева відмов" і способу оцінки показника чистої приведеної вартості проекту розроблення безпечного ПЗ з урахуванням негативних факторів можливого невиявлення загроз безпеки ПЗ.

У третьому розділі удосконалено метод оптимізації розподілу ресурсів розроблення програмного забезпечення в умовах підвищених вимог щодо захисту інформації. В основу цього методу була покладена напівмарківська модель розподілу ресурсів проектування ПЗ для керованого марківського процесу у безперервному часі.

Використовувані в даному розділі теоретичні положення в достатньому об'ємі відбивають стандарти і можливості сучасних методологій тестування ПЗ.

У четвертому розділі дисертаційної роботи розроблено математичні моделі технології тестування комплексу *DOM XSS* вразливостей і технології тестування вразливості до *SQL*-ін'єкцій.

Математична модель технології тестування комплексу *DOM XSS* вразливостей відрізняється від відомих урахуванням специфіки комплексного аналізу різних типів *XSS* уразливості ("*stored XSS*", "*reflected XSS*" і *DOM Based XSS*), а також включенням в алгоритм процедур автоматичного аудиту *DOM Based XSS* окремо.

Математична модель технології тестування вразливості до *SQL*-ін'єкцій відрізняється від відомих вдосконаленим способом визначення відстані між результатами ін'єкції.

У п’ятому розділі отримано подальший розвиток імітаційна модель технології тестування безпеки. Відмінною особливістю розробленої імітаційної моделі є адаптація вибору вхідних операторів управління і даних до підвищення вимог оперативності розроблення і реалізації моделі, виражена в реалізації процедури взаємодії з реальним браузером з використанням засобів автоматизації браузеру і формуванні даних для атаки на декількох діалектах.

Основною метою шостого розділу є розробка та обґрунтування практичних рекомендацій з використання методів та засобів управління безпекою ПЗ, а також оцінка достовірності отриманих результатів математичного моделювання.

Наукова новизна дисертаційної роботи.

1. *Удосконалено* метод якісного аналізу вразливостей розроблення програмного забезпечення, що відрізняється від відомих врахуванням факторів експлуатаційних вразливостей, особливо вразливості невиявлення загроз безпеки ПЗ КС, і оцінкою довільного несуперечливого кінцевого набору «квантів інформації», це дозволяє звузити множину важливих вразливостей і знизити можливі фінансові та іміджеві втрати організацій-розробників ПЗ.

2. *Удосконалено* метод кількісної оцінки вразливостей розроблення ПЗ, що відрізняється від відомих комплексним використанням методики «Аналізу дерева відмов» і способу оцінки показника чистої приведеної вартості проекту розроблення безпечного ПЗ з урахуванням негативних факторів можливого невиявлення загроз безпеки ПЗ КС, це дозволило підвищити точність кількісної оцінки вразливостей розроблення ПЗ.

3. *Удосконалено* метод оптимізації розподілу ресурсів розроблення ПЗ на основі напівмарківської моделі прийняття рішень для керованого марківського процесу у безперервному часі. Відмінною особливістю запропонованого методу є використання псевдобулевих методів бівалентного програмування з нелінійною цільовою функцією і лінійними обмеженнями для визначення оптимальної стратегії усунення експлуатаційних помилок, це дозволяє оптимізувати процес проектування стратегії розподілу ресурсів розроблення ПЗ.

4. *Вперше розроблено* математичну модель технології тестування комплексу *DOM XSS* вразливостей, яка за рахунок урахування специфіки комплексного аналізу різних типів *XSS* вразливості («*stored XSS*», «*reflected XSS*» і *DOM Based XSS*), а також включенням в алгоритм процедур автоматичного аудиту *DOM Based XSS* окремо, дозволяє провести аналітичну оцінку часових витрат тестування вказаних вразливостей в умовах реалізації стратегії розроблення безпечного програмного забезпечення.

5. *Вперше розроблено* математичну модель технології тестування вразливості до *SQL*-ін'єкцій, яка за рахунок використання критерію Джаро-Вінклера, для порівняння результатів ін'єкції *SQL*-коду і введення порогового значення дозволяє підвищити точність результатів тестування безпеки програмного забезпечення.

6. *Вперше розроблено* метод математичного моделювання технологій тестування *DOM XSS* вразливості та вразливості до *SQL*-ін'єкцій, в основу якої покладений підхід мережевого *GERT* моделювання, це дозволило досліджувати процеси в комп'ютеризованих системах при розробці нових засобів і протоколів

захисту даних, а також зменшити час тестування безпеки програмного забезпечення.

7. *Отримано подальший розвиток* імітаційної моделі технології тестування безпеки на основі положень теорії масштабування імітаційних моделей. Відмінною особливістю розробленої імітаційної моделі є адаптація вибору вхідних операторів управління і даних до підвищення вимог оперативності розроблення і реалізації моделі, виражена в реалізації процедури взаємодії з реальним браузером, з використанням засобів автоматизації браузеру і формуванні даних для атаки на декількох діалектах, це дозволило понизити обчислювальну складність алгоритмів, що реалізовуються.

8. *Вперше розроблено* метод передтестової компіляції і розподілу доступу, який за рахунок врахування профілів користувача при розроблені застосунку, а також використання ресурсів «хмарних сховищ» в процесі отримання інсталяційних версій дозволяє підвищити рівень безпеки застосунків, що розробляються.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність.

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується аргументованими результатами досліджень, співставленням з результатами математичного моделювання, великою кількістю апробацій та публікацій.

Практичне значення отриманих результатів в області розроблення ПЗ полягає в тому, що запропоновані в дисертаційній роботі моделі та методи є науково-методичною основою для розроблення відповідних компонентів програмних продуктів, алгоритмів, системних утиліт та протоколів. Практична значущість отриманих результатів полягає в наступному:

– метод якісного аналізу вразливостей розроблення ПЗ дозволив на 55% звузити сукупність множин Парето та більш точно обирати пріоритетність напрямків фінансування профілактичних заходів;

– метод кількісної оцінки вразливостей розроблення ПЗ дозволив за рахунок використання удосконаленої методики "Аналізу дерева відмов" підвищити точність кількісної оцінки вразливостей розроблення ПЗ до 20% та спроектувати програмну систему оцінки чистої приведеної вартості проекту розроблення безпечного ПЗ;

– метод математичного моделювання технологій тестування *DOM XSS* вразливості та вразливості до *SQL*-ін'єкцій дозволив розробити автоматизований програмний засіб виявлення вразливості ПЗ, що дає можливість зменшити час тестування безпеки від 1,05 до 1,5 разів.

Практична значущість отриманих результатів підтверджується їх застосуванням:

– при розробці автоматизованих систем виявлення вразливостей ПЗ Інтернет сервіс провайдері ТОВ «ІМПЕРІАЛ-НЕТ» (м. Кропивницький);

– удосконаленні гнучкої методології розроблення ПЗ у компанії-розробнику програмного забезпечення ТОВ «МІФ ПРОДЖЕКТС» (м. Кропивницький);

– при розробці систем захисту інформації ТОВ «САЙФЕР ІТ» (м. Київ);

– у навчальному процесі Центральноукраїнського національного технічного університету.

Апробація результатів роботи та публікації.

Основні положення дисертаційної роботи були представлені на наступних конференціях: «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ, 2016-2018 рр.); «*Securitea informationala*» (*Chisinau*, *Moldova*, 2016-2018 рр.); «Інформатика та системні науки» (Полтава, 2016 р.); «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (Київ, 2016-2017 рр.); «Інформаційна безпека та комп'ютерні технології» (Кропивницький, 2016-2018 рр.); «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі» (Харків, 2016-2017 р.);

«Комбінаторні конфігурації та їх застосування» (Кропивницький, 2016-2017 рр.); «Проблеми і перспективи розвитку ІТ-індустрії» (Харків, 2016-2018 рр.); «Інформаційна та економічна безпека» (Харків, 2016 р.); «Стратегия качества в промышленности и образовании» (Варна, Болгарія, 2016, 2018 рр.); «Кібербезпека в Україні: правові та організаційні питання» (Одеса, 2016 р.); «Актуальні задачі та досягнення у галузі кібербезпеки» (Кропивницький, 2016 р.); «*Information technologies, systems and networks*» (*Chisinau*, *Moldova*, 2017 р.); «Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті» (Кропивницький, 2017 р.); «Комп'ютерні інтелектуальні системи та мережі» (Кривий Ріг, 2018 р.); «Комп'ютерна інженерія і кібербезпека: досягнення та інновації» (Кропивницький, 2018 р.).

Основні положення і результати дисертації опубліковано у 59 наукових працях, у тому числі: 1 монографія; 3 колективні монографії; 2 наукові статті у міжнародних рецензованих виданнях, що входять до бази даних Scopus; 3 наукові статті у закордонних фахових наукових журналах, та 22 статті у наукових журналах та збірниках наукових праць, що входять до переліку фахових видань України (з них без співавторів – опубліковано 16), а також 28 матеріалів і тез доповідей на всеукраїнських та міжнародних конференціях.

Відповідність автореферату дисертації. Зміст автореферату є ідентичним до змісту дисертації й повною мірою відображає основні завдання, наукову новизну, практичне значення, висвітлює всі отримані результати, висновки та запропоновані рекомендації.

Зауваження по роботі:

1. В другому розділі відсутні оцінки значень ймовірностей виникнення вразливостей, які є елементами дерева вразливостей розроблення програмного забезпечення (Таблиця 2.6., стор. 115)

2. В третьому розділі відсутня постановка оптимізаційної задачі та формальне подання методу розподілу ресурсів розроблення безпечного

програмного забезпечення, наведено лише практичні рекомендації щодо застосування даного методу (п. 3.4.)

3. У четвертому розділі при розробці комплексу математичних моделей процесу тестування Web-застосунків автор застосовує твірну функцію моментів експоненційного розподілу. Це є спрощений погляд на процес тестування в цілому та окремі етапи тестування зокрема. Доцільно було б використовувати інші, більш складні, закони розподілу, або методи формалізації з використанням нечіткої логіки.

4. При Gert-моделюванні технології тестування комплексу *DOM XSS* вразливостей та Gert-моделюванні технології тестування вразливості до *SQL*-ін'єкцій автор знаходить корені поліномів 4.8. та 4.17 відповідно. Нажаль в подальшому автор не вказує можливі впливи різноманіття рішень на загальний вигляд кінцевого результату.

5. Запропоновані у четвертому розділі моделі формалізують лише окремі види тестування безпеки програмного забезпечення. Автору було б доцільно запропонувати загальну модель тестування на проникнення з врахування окремих етапів експертного, динамічного та статичного аналізу програмного забезпечення.

6. При наданні рекомендацій практичного використання моделей та методів розроблення безпечного програмного забезпечення автор нажаль не в повному обсязі враховує опит звісних світових практик (наприклад опит CERT), пов’язаних з реалізацією та верифікацією безпечного програмного забезпечення. Зокрема не враховуються парадигми моделі AIR, Source Code Analysis Laboratory (SCALe), нечіткого тестування та ін.

Відзначені зауваження не ставлять під сумнів основні наукові та практичні результати, і суттєво не впливають на загальну позитивну оцінку дисертаційної роботи.

Висновок.

Дисертаційна робота Коваленка Олександра Володимировича представляє собою завершене актуальне наукове дослідження. В роботі отримано нові

наукові результати, які дозволяють розвинути наукові методики та технології ідентифікації стану в комп'ютерних та комп'ютеризованих системах.

Вважаю, що докторська дисертація Коваленка Олександра Володимировича за актуальністю теми, ступенем обґрунтованості наукових положень, рівнем апробації та публікацій, науковою новизною та практичною цінністю отриманих результатів відповідає вимогам, що висуваються до докторських дисертацій згідно п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а сам автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
професор кафедри математичних методів системного аналізу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
доктор технічних наук, професор

В.Є. Мухін

Підпис професора кафедри математичних методів системного аналізу
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
д. т. н., проф. Мухіна В.Є. засвідчую:

Вчений секретар
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»,
кандидат технічних наук, доцент

В. В. Холявко