До спеціалізованої вченої ради Д 73.052.04
у Черкаському державному технологічному університеті
18006, м. Черкаси, бул. Шевченка, 460.

ВІДГУК

офіційного опонента Чемериса Олександра Анатолійовича
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.

На теперішній час використання програмних платформ комп'ютерних систем (КС) внаслідок своєї специфіки характеризується розвитком численних форм ризику та їх особливим характером протікання. При цьому експлуатація таких складних програмних систем на сучасному етапі усе більшою мірою стикається з проблемами забезпечення інформаційної безпеки. Крім цього, збільшення попиту та вартості інформаційних ресурсів, а також тяжкий характер їх пошкодження або знищення збільшує актуальність цього питання. Одним з можливих шляхів вирішення проблем забезпечення безпеки програмних застосунків КС в умовах зовнішніх впливів є синтез нових моделей та методів розроблення безпечного програмного забезпечення.

Формалізація процесу розроблення безпечного програмного забезпечення (ПЗ) становить складне завдання зважаючи на значну різноманітність, складність математичного опису, а також невизначеність вхідних даних при використанні гнучких методологій розроблення програмного забезпечення.

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 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 аналіз основних тенденцій розвитку моделей та методів розроблення безпечного програмного забезпечення і вимог до програмних засобів. Наведено результати досліджень сучасних моделей та методів розроблення безпечного програмного забезпечення і факторів, що впливають на безпеку. Проведено аналіз і порівняльне дослідження основних підходів математичного моделювання процесу розроблення безпечного програмного забезпечення. На основі виявлених закономірностей, переваг і недоліків сучасних методологій розроблення безпечного програмного забезпечення здійснюється постановка завдання дисертаційного дослідження.

У другому розділі дисертаційної роботи удосконалено методи якісного аналізу і кількісної оцінки вразливостей розроблення програмного забезпечення, що дозволило вирішити протиріччя, що виникають при розробці ПЗ, і які полягають у зневазі фірмами-розробниками ПЗ факторами вразливості

безпеки ПЗ. В якості вирішення вказаної проблеми запропоновано використання розроблених методів якісного аналізу і кількісної оцінки вразливостей розроблення програмного забезпечення.

Удосконалено 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".

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

У третьому розділі розглянуто задача оптимізації розподілу ресурсів розроблення ПЗ за умови обмеженості ресурсів (фінансових, технічних та ін.), які маються у наявності на усунення помилок безпеки. Процес розглядається як напівмарківська модель прийняття рішень для керованого процесу у безперервному часі з критерієм мінімуму витрат на усунення аномалій.

Удосконалено метод оптимізації розподілу ресурсів розроблення ПЗ, що відрізняється від відомих використанням псевдобулевих методів бівалентного програмування з нелінійною цільовою функцією і лінійними обмеженнями для визначення оптимальної стратегії усунення експлуатаційних помилок.

У якості прикладу розглянуто ситуації виникнення помилок безпеки ПЗ і визначено оптимальну стратегію управління для усунення вказаної аномальної ситуації.

У четвертому розділі дисертаційної роботи представлено результати дослідження і алгоритми тестування на вразливість до одних з найбільш поширених видів атак на *Web*-застосунки – *DOM XSS* і *SQL*-ін'єкції.

Розроблено комплекс математичних моделей процесу тестування *Web*-застосунків. В основу математичного моделювання покладено підхід мережевого *GERT* моделювання. В результаті 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.

П'ятий розділ присвячено розробці імітаційної моделі технології тестування безпеки на основі положень теорії масштабування імітаційних моделей, що відрізняється від відомих адаптацією вибору вхідних операторів управління і даних до підвищення вимог оперативності розроблення і реалізації моделі, яке виразилося 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 проведено дослідження ефективності розроблених моделей і методів тестування безпеки застосунків, оцінку достовірності отриманих результатів математичного моделювання, а також обґрунтування практичних рекомендацій з використання методів та засобів управління безпекою.

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 коректним використанням відповідного математичного апарату і підтверджується співставленням з результатами експериментальних досліджень.

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 (Додаток А):

– 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. У першому розділі автор наводить дуже стислий перелік методів математичної формалізації процесу розробки безпечного програмного забезпечення. Доцільно було б розглянути можливості використання інтелектуальних методів математичного моделювання, особливо з урахуванням нечіткості вхідних даних.

2. У другому розділі при розробці методу якісного аналізу вразливостей розроблення програмного забезпечення автор пропонує вирішити завдання вибору несуперечливих "квантів інформації". Також наводить практичний приклад вирішення цього завдання. Нажаль дослідження щодо точності отриманих результатів та їх достовірності проведено не було.

3. При розробленні оптимізаційної марківської стаціонарної стратегії розподілу ресурсів проектування безпечного ПЗ автор вводить гіпотезу про лінійність обмежень. При цьому аргументу саме цього класу обмежень автор не наводить. В той же час складний характер процесу розроблення ПЗ наводить на висновок про більш неоднозначний клас існуючих обмежень моделювання.

4. При розробленні оптимізаційної стратегії напівмарківської моделі розподілу ресурсів проектування безпечного ПЗ автор нажаль не запропонував

рішення визначення ймовірностей перебування об'єктів у будь який час, що в деякій мірі зменшило практичну значущість результатів моделювання.

5. При розробці комплексу математичних моделей процесу тестування Web-застосунків автор пропонує використовувати методи GERT-мережевого моделювання. Але нажаль при цьому автор не враховує можливу нечіткість вхідних даних.

6. Для оцінки ефективності синтезованих моделей та методів розроблення безпечного ПЗ, а також аналізу результатів тестування безпеки *Web*-застосунків автор бере як приклад програмне забезпечення комп'ютерної системи управління інформаційними потоками авіатранспортного підприємства (КСУ ІП АП). Нажаль автор при цьому не привернув уваги на те що програмне забезпечення для систем критичного застосування на даний час розробляється за допомогою «водоспадної» методології, що має відмінності у порівнянні з гнучкими методологіями.

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

Висновок.

Дисертаційна робота Коваленко Олександра Володимировича представляє собою завершене актуальне наукове дослідження. В роботі отримано нові науково- обґрунтовані результати, які дозволяють розвинути наукові методики та технології ідентифікації стану в комп'ютерних та комп'ютеризованих системах.

Вважаю, що докторська дисертація Коваленко 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:
заступник директора з наукової роботи
Інституту проблем моделювання в
енергетиці ім. Г.Є. Пухова НАН України,
д-р техн. наук, ст.наук. співроб. О.А. Чемерис

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ім. Г.Є.Пухова
Ідентифікаційний код 05516949
м.Київ