Голові разової спеціалізованої
вченої ради PhD 9279
Хмельницького національного університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО

ВІДГУК

офіційного опонента на дисертаційну роботу
Регіди Павла Геннадійовича
на тему: «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання», представлену на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації. Поточна ситуація з поширенням зловмисного програмного забезпечення (ЗПЗ) визначає серйозні виклики щодо захисту інформації користувачів. Попри наявність різноманітних антивірусних програмних засобів (АПЗ), динаміка появи нових екземплярів ЗПЗ свідчить про актуальність пошуку нових методів їх виявлення. Розробники ЗПЗ активно вивчають методи виявлення, які реалізовані в сучасних АПЗ та впроваджують методи уникнення виявлення. Також, зловмисники вдаються до модифікації відомих програм, наділяючи її властивостями притаманними ЗПЗ, формуючи таким чином інфіковані програми (ІП). Практика поширення сформованих ІП дозволяє підвищувати шанси на проникнення в цільову систему, навіть із використанням АПЗ, зловмисного коду, що і становить загрозу для даних користувачів.

Із метою захисту від подібних загроз фахівцями з кібербезпеки було запропоновано низку рішень – як таких, що використовуються безпосередньо на користувацьких хостах, так і комплексних систем, розгорнутих у межах корпоративних мереж. В обох випадках під час виявлення різних типів ЗПЗ застосовується концепція пісочниці та емуляції виконання програм, що, з одного боку, забезпечує високі шанси виявлення, а з іншого – гарантує безпечність аналізу завдяки використанню ізольованого середовища виконання. Зважаючи на те, що сучасні екземпляри ЗПЗ поєднують різні методи уникнення виявлення та потребують детального аналізу, а в окремих випадках – багаторазового аналізу поведінки виконання в різних умовах виконання, залучення розподілених систем, здатних забезпечити необхідний обсяг обчислювальних ресурсів, є актуальним напрямком досліджень.

Усе вищезазначене зумовлює актуальність теми дисертаційної роботи Регіди П.Г., яка присвячена розв'язанню важливої науково-прикладної задачі, пов'язаної з організацією грід-обчислювальних систем для виявлення зловмисної поведінки в інфікованих програмах на основі аналізу їх виконання в модифікованих ізольованих середовищах.

Зв'язок роботи з науковими програмами, планами темами. Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем Хмельницького національного університету. Її зміст відповідає тематиці науково-дослідних робіт за держбюджетними темами Хмельницького національного університету «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (номер держреєстрації 0121U109936), «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер держреєстрації 0124U000980).

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1) вперше розроблено модель централізованих грід-обчислювальних систем, в якій враховано вимоги до залучення автономних та гетерогенних обчислювальних елементів для забезпечення виконання задач із перевіркою на коректність в динамічному середовищі виконання, і яка дає змогу залучити під'єднані обчислювальні елементи для аналізу поведінки виконання інфікованих програм, забезпечуючи розподілений процес виявлення зловмисного прояву в інфікованих програмах;

2) розроблено новий метод синтезу засобів формування шаблонів поведінки інфікованих програм, який на відміну від відомих відрізняється залученням пісочниці для їх виконання у наборі створюваних модифікованих ізольованих середовищах за допомогою виконання програмних переривань та базового емулятора із визначеним набором реалізованих низькорівневих інструкцій, що дає змогу отримувати з них шаблони поведінки на множинах станів емульованих центральних процесорів з метою виявлення зловмисної поведінки з урахуванням особливостей методів уникнення від виявлення, які реалізовані зловмисниками;

3) удосконалено метод організації функціонування грід-обчислювальних систем, який на відміну від відомих залучає жадібний алгоритм для оптимізації навантаження між автономними гетерогенними обчислювальними елементами та використовує додаткову чергу активних задач, що дає змогу забезпечити збалансоване виконання поставлених задач в розподілених системах із динамічно змінюваною топологією для розподіленого виявлення зловмисної поведінки в інфікованих програмах;

4) удосконалено метод оцінювання довіри автономних обчислювальних елементів, який на відміну від відомих використовує

механізми призначення ролей із використанням елементів нечіткої логіки, що дає змогу оптимізувати використання обчислювальних ресурсів шляхом скорочення кількості повторних обчислень у системах, що функціонують в динамічному середовищі.

Наукові положення, висновки і рекомендації дисертаційної роботи Регіди П.Г. достатньо обґрунтовані коректним використанням математичного апарату, підкріплені успішною реалізацією, ефективним практичним впровадженням результатів дисертаційних досліджень, яке продемонструвало відповідність теоретичних досліджень із одержаними результатами. При розв'язанні поставленої науково-прикладної задачі використовувались теорії абстрактної алгебри для визначення архітектури грід-обчислювальних систем, теорії множин і графів для визначення інфікованих програм, теорії розподілених систем для організації її функціонування та методи уникнення виявлення інфікованих програм.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою і базується на детальному аналізі джерел за даною проблематикою, чіткій постановці задач дослідження, використання новітніх методів дослідження, правильним застосуванням математичного апарату при теоретичному розгляді наукових положень дисертації, а також проявляється у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів, які були використані під час виконання роботи.

Наукові положення, висновки та рекомендації, сформульовані в дисертації, логічно випливають із результатів, одержаних за допомогою чітких викладок. Тому, можна вважати, що висновки та практичні рішення, одержані у роботі достатньо обґрунтовані і коректні.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, здобувач повною мірою оволодів методологією наукової діяльності.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності. За своїм змістом дисертаційна робота здобувача Регіди П.Г. повністю відповідає Стандарту вищої освіти зі спеціальності 123 Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти та освітньо-науковій програмі ХНУ «Комп'ютерна інженерія» за спеціальністю 123 Комп'ютерна інженерія. Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерної інженерії.

Розглянувши результати перевірки дисертаційної роботи, можна зробити висновок, що дисертаційна робота Регіди Павла Геннадійовича є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідне джерело.

Практичне значення одержаних результатів. Результатом дисертаційної роботи є розроблена централізована грід-обчислювальна система для виявлення зловмисної активності в інфікованих програмах. Система використовує синтезовані засоби формування поведінки виконання інфікованих програм, які розгортаються на підключених обчислювальних елементах. Для виявлення зловмисної поведінки застосовується множина модифікованих ізольованих середовищ виконання, які формуються із урахуванням проаналізованих методів протидії емуляції, що використовуються в сучасних екземплярах інфікованих програм. Тому, ці середовища виконання виступають у ролі пасток, які проковують зміну поведінку виконання. З метою ефективного використання ресурсів автономних та гетерогенних обчислювальних елементів у системі реалізовано удосконалений метод розподілу задач. Крім того, для

зменшення кількості повторних обчислень, необхідних для забезпечення коректності виконання завдань, удосконалено метод оцінки довіри до обчислювальних елементів. Цей метод ґрунтується на рольовій моделі з урахуванням поведінкових характеристик елементів під час їх функціонування в системі.

Результати дисертаційної роботи впроваджено у ТОВ «Nolt technologies» (м. Хмельницький), ТОВ «ІТТ» (м. Хмельницький), а також в освітньому процесі Хмельницького національного університету.

Мова та стиль викладення результатів. Дисертаційна робота написана українською мовою. Дисертація написана логічно, доступно на високому технічному рівні з використанням сучасної термінології. Матеріали дисертаційної роботи викладено послідовно, доступно для розуміння і сприйняття. Стиль мовлення задовольняє вимоги до текстів науково-технічного змісту. Текст дисертації в достатній мірі проілюстрований таблицями та рисунками. Здобувач використовує загальноприйняту термінологію.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох додатків. Повний обсяг роботи містить 190 сторінок друкованого тексту, з них анотація – на 10 стор., зміст – на 2 стор., перелік умовних скорочень – на 1 стор., основний текст – на 129 стор., список із 131 використаних джерел – на 17 стор., додатки – на 28 стор. Дисертація містить 27 рисунків та 10 таблиць.

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Оприлюднення результатів дисертаційної роботи. Основні результати дисертації опубліковані в 11 наукових працях, серед яких 4 статті у фахових наукових журналах України, включених на дату опублікування до

переліку наукових фахових видань України категорії Б; 6 праць в матеріалах міжнародних та всеукраїнських конференцій (4 з яких проіндексовано у наукометричній базі Scopus); 1 свідоцтво про реєстрацію авторського права на твір.

У підсумку, опубліковані праці віддзеркалюють повноту викладу результатів дисертаційної роботи. Науковий рівень публікацій – високий. У всіх публікація здобувачем дотримано принципів академічної доброчесності.

Таким чином, наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи:

1. У першому розділі дисертаційної роботи не було розглянуто інших класів алгоритмів планування обчислень в грід-обчислювальних системах, окрім як жадібних.

2. При визначенні ефективності грід-обчислювальної системи доцільно також враховувати показники, що характеризують аварійне відключення обчислювальних елементів під час виконання робочої ітерації.

3. В основу роботи взято інфіковані програми, які використовують частину проаналізованих методів протидії емуляції з метою уникнення виявлення. Водночас у роботі відсутній деталізований опис їх одночасного застосування в межах одного екземпляра інфікованої програми.

4. У методі організації функціонування розподіленої системи (розділ 3.2, крок 3) запропоновано на початку робочої ітерації виконувати сортування всіх підзадач за спаданням складності обчислень. За такого підходу існує ймовірність, що підзадачі з меншою складністю залишатимуться невиконаними, оскільки вони можуть не бути розподілені між підключеними обчислювальними елементами на початковому етапі робочої ітерації.

5. У роботі представлено дві множини поведінкових характеристик кожного обчислювального елемента, які згодом використовуються для виявлення скомпрометованих елементів. Водночас не запропоновано жодних механізмів додаткової верифікації користувача у разі зміни апаратного забезпечення, що може призвести до неефективного використання його обчислювальних ресурсів.

6. На сторінці 48, у реченні щодо використання статичних алгоритмів в умовах динамічно змінюваної топології, доцільніше було б замінити слово «від'єднати» на «відключити». У реченні «Так як виконання ІП чутливе особливостей середовища виконання» (сторінка 91) пропущено прийменник «до». Крім того, у тексті виявлено незначну кількість граматичних та орфографічних помилок, зокрема на сторінках 66, 85 та 104.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

Висновок про дисертаційну роботу. Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Регіди Павла Геннадійовича на тему «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 6-9 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами, внесеними згідно з Постановами Кабінету

Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024).

Здобувач Регіда Павло Геннадійович заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент
доктор технічних наук, професор
завідувач кафедри електронних обчислювальних машин
Харківського національного університету радіоелектроніки

Андрій КОВАЛЕНКО

ПІДПИС ЗАСВІДЧУЮ
Ректор
Харківського національного університету радіоелектроніки
доктор технічних наук, професор

Ігор РУБАН

"17" червня 2025 р.