Голові разової спеціалізованої
вченої ради PhD 9279
Хмельницького національного університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА
доктора технічних наук, професора **Возної Наталії Ярославівни**
на дисертаційну роботу **Регіди Павла Геннадійовича**
на тему: «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання», подану до захисту на здобуття наукового ступеня **доктора філософії** з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи

Інформаційні технології сьогодні знаходять своє використання в багатьох сферах діяльності, забезпечуючи автоматизацію рутинних операцій. Це забезпечується активним використанням програмних застосунків (ПЗ), які можуть використовуватись зловмисниками для отримання конфіденційних даних, за допомогою використання зловмисного програмного забезпечення (ЗПЗ). Розробники ЗПЗ активно досліджують сучасні методи виявлення, які використовуються в антивірусних програмних засобах (АПЗ), що дозволяє реалізовувати методи уникнення виявлення та стратегії їх застосування. Такі методи і стратегії є частиною інфікованих програм (ІП), що поширюються з метою прихованого виконання зловмисних дій. Сукупність усіх цих факторів, а також і те, ІП набувають і поліморфних властивостей свідчить про суттєві виклики у сфері захисту інформації користувачів.

Після інфікування цільова програма набуває властивостей, що дозволяють їй змінювати власну поведінку, знижуючи ймовірність виявлення під час аналізу засобами АПЗ. Тому, важливим завданням є розробка засобів і методів, що забезпечать формування поведінки інфікованої програми, на основі якого буде проводитись її аналіз на наявність зловмисної поведінки. До таких засобів відносять такі, що використовують технології емуляції виконання програм та створення ізольованого середовища виконання, а їх комплексне застосування дозволяє безпечно формувати поведінку виконання ІП.

Одним із недоліків використання емуляції визначають збільшене використання ресурсів, які потребуються на виконання тієї самої програми, у порівнянні із її виконанням в середовищі без застосування емуляції.

Зважаючи також на стрімке кількісне та якісне зростання ЗПЗ із кожним роком, а також необхідність у застосуванні комплексних перевірок різних екземплярів інфікованих програм, застосування розподілених систем є провідним підходом для вирішення визначеної задачі з виявлення зловмисної поведінки.

Отже, розроблення методів та засобів для покращення ефективності функціонування грід-обчислювальної системи для виявлення зловмисної поведінки в ІП на основі поведінки виконання в модифікованих ізольованих середовищах виконання є актуальною науково-прикладною задачею.

2. Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету: держбюджетної науково-дослідної теми №1Б-2021 «Самоорганізована розподілена система виявлення зловмисного програмного забезпечення в комп'ютерних мережах» (номер держреєстрації 0121U109936); держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер держреєстрації 0124U000980), в яких автор дисертації був виконавцем.

3. Наукова новизна отриманих результатів.

До основних наукових результатів дисертаційної роботи варто віднести:

- вперше розроблено архітектуру грід-обчислювальної системи, яка використовує автономні та гетерогенні обчислювальні елементи для формування поведінки виконання інфікованих програм в модифікованих ізольованих середовищах, що дозволить забезпечити розподілений процес виявлення зловмисної поведінки в інфікованих програмах.
- розроблено новий метод синтезу системи засобів формування шаблону поведінки у визначених умовах виконання, які включають пісочницю для створення модифікованого ізольованого середовища виконання та базового емулятора із визначеним набором низькорівневих інструкцій, що дає можливість виявляти зловмисну поведінку.
- удосконалено метод організації обчислень в розподіленій грід системі, що базується на використанні жадібного алгоритму для оптимізації навантаження між гетерогенними обчислювальними елементами, а також додаткову чергу задач що забезпечує правильність виконання аналізу інфікованих програм враховуючи динамічність середовища функціонування системи.
- удосконалено метод оцінювання довіри автономних обчислювальних елементів використанням елементів нечіткої логіки для визначення їх ролі, що дозволило скоротити кількість повторних обчислень в системі.

4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації адекватно і в повній мірі відображає її зміст.

У *вступі* обґрунтовано актуальність теми дисертації, визначено мету, предмет та об'єкт дослідження, визначені основні завдання, відображено наукову новизну і практичне значення одержаних результатів.

У *першому розділі* здійснено аналіз предметної області дослідження, існуючих комерційних програмних систем і застосунків та їх методів функціонування, що використовуються для виявлення зловмисної поведінки в інфікованих програмах. Також проведено аналіз існуючих підходів організації розподілених обчислювальних систем та особливості їх функціонування.

У *другому розділі* представлено модель інфікованої програми, яка включає її властивості виконання в середовищі виконання із урахуванням методів уникнення виявлення, що включають протидію емуляції та обфускації. Розроблено архітектури засобів, які використовуються для формування поведінки виконання і базуються на технологіях пісочниці та емулятора. Розроблено архітектуру програмної частини центрального сервера розподіленої системи, що залучає представлені засоби формування поведінки виконання. Усі представлені архітектури подані графічно із урахуванням їхніх компонентів та функцій. Розроблено також і модель розподіленої системи виявлення зловмисної поведінки в інфікованих програмах, що залучає розроблені архітектури та їх функціональні особливості.

У *третьому розділі* представлено метод, за допомогою якого відбувається синтез засобів формування шаблонів поведінки, що базується на використанні модифікованих ізольованих середовищ та емулятора із визначеним набором низькорівневих інструкцій. Також, представлено метод для оптимізації використання обчислювальних ресурсів підключених гетерогенних обчислювальних елементів, який використовує жадібний алгоритм та додаткову чергу виконання. Додатково, представлена реалізація удосконаленого методу оцінювання довіри підключених обчислювальних елементів для оптимізації кількості необхідних повторних обчислень на основі рольової моделі в динамічному середовищі функціонування системи.

У *четвертому розділі* представлено опис розроблених програмних частин центрального серверу та обчислювального елемента, деталізовано подано особливості їх реалізації, та частково описано розроблений мережевий протокол обміну даними між елементами системи. Також представлені проведені експерименти, описано умови їх проведення та проведено аналіз отриманих результатів.

У *висновках* подано отримані основні наукові та практичні результати дослідження.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність.

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими і підкріплені практичною реалізацією.

Наукова обґрунтованість положень і висновків дисертації забезпечена аналізом літературних джерел, чітким формулюванням завдань дослідження та використанням сучасних методологічних підходів.

Достовірність одержаних результатів підтверджена їх апробацією на міжнародних та всеукраїнських наукових конференціях, а також практичним впровадженням.

6. Практичні результати роботи

В представленій роботі реалізована система виявлення інфікованих виконуваних програм що використовують методи уникнення виявлення, а саме: протидії емуляції та обфускації. Запропонована централізована грід-обчислювальна система використовує залучені обчислювальні елементи для розгортання синтезованих засобів формування поведінки інфікованих програм для виявлення зловмисної прояву. Запропонований метод виявлення ІП базується на використанні досліджених методів протидії емуляції, і використовує їх теоретичні засади для формування пасток у вигляді модифікованих ізольованих середовищ виконання. Реалізовані методи підвищення ефективності функціонування стосуються зменшення часу роботи системи та кількості необхідних повторних обчислень завдяки представленим відповідним удосконаленими методам. Реалізований метод виявлення зловмисної поведінки в ІП демонструє успішність в більшості випадків 98-99%, при виконанні аналізу згенерованих сімейств моделей ІП на основі досліджених технік протидії емуляції.

У результаті проведених експериментальних досліджень було підтверджене коректне функціонування централізованої грід-обчислювальної системи виявлення зловмисної поведінки в ІП.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «Nolt technologies» (м. Хмельницький), ТОВ «ІТТ» (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університет при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності 123 Комп'ютерна інженерія, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Безпека та захист комп'ютерних систем», «Комп'ютерні мережі, системне адміністрування та кібербезпека».

7. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях.

Дисертаційна робота має логічну структуру і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та чотирьох додатків. Повний обсяг роботи становить 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. Оформлення дисертації відповідає необхідним вимогам.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами досліджень опубліковано 4 статті у наукових фахових виданнях, одне свідоцтво про реєстрацію авторського права на твір (програму), 6 тез доповідей у збірниках матеріалів конференцій, з яких 4 праці індексовані в наукометричній базі Scopus.

Усі сформовані наукові положення і результати дисертації повністю викладено в опублікованих працях.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності. Дисертація містить достатню кількість ілюстративного матеріалу – схем, рисунків, графіків і таблиць. Мова викладу, стиль та оформлення роботи повністю відповідають установленим вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

Зауваження та рекомендації до дисертації

- У першому розділі дисертаційної роботи не було повною мірою розглянуто основні підходи до виявлення поліморфних вірусів у складі проаналізованих програмних антивірусних застосунків і систем.

-Запропонована грід-обчислювальна система, за умови підключення великої кількості обчислювальних елементів, може потребувати значних обчислювальних ресурсів з боку центрального сервера, що, у свою чергу, може спричинити затримки під час передавання завдань обчислювальним елементам для формування поведінкових профілів виконання інфікованих програм.

- У розділі 3.1, присвяченому синтезу засобів формування поведінки виконання інфікованої програми, в кроці 4.3 представлено перетворення, що стосуються врахування змін стану регістрів і пам'яті програми. У випадку з регістрами алгоритм формування поведінки враховує їх зміну протягом усього часу виконання програми, тоді як для пам'яті програми, згідно із описом алгоритму, враховується лише фінальний стан після завершення виконання програми.

- Запропонований метод виявлення не враховує поліморфні віруси третього класу, які за певними ознаками до можуть бути помилково віднесені до другого класу, зважаючи на те, що основна відмінність між другим і третім класами полягає у ступені деталізації їх характерних особливостей.

- В поданому мережевому протоколі (Розділ 4, Рис. 4.7) наведено сервісні повідомлення, зокрема ті, що використовуються для перевірки доступності обчислювальних елементів. Водночас не було детально розкрито, яким чином змінюється алгоритм функціонування під час виконання робочої

ітерації центрального сервера у випадках, коли окремі обчислювальні елементи стають недоступними.

На сторінках 36-38 трапляються терміни «дебагінг», «проксування», «руткіт» та «патерн», для яких здобувачу доцільно надалі використовувати українські відповідники та уникати вживання англіцизмів. Крім того, у тексті дисертаційної роботи виявлено незначну кількість граматичних та орфографічних помилок, зокрема на сторінках 93, 94 та 104.

Зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Регіди Павла Геннадійовича на тему «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання», що подана на здобуття ступеня доктора філософії, за своїм науковим рівнем та практичною цінністю, змістом та оформленням повністю відповідає вимогам пп. 6, 7, 8, 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, а її автор, Регіда Павло Геннадійович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Офіційний опонент –
доктор технічних наук, професор,
професор кафедри спеціалізованих
комп'ютерних систем,
Західноукраїнський національний
університет Наталія ВОЗНА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ * 33680120 *

Підпис Наталія Возна
Завіряю:
НАЧАЛЬНИК
ЗАГАЛЬНОГО ВІДДІЛУ Анна Семик