Зразок_1

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання»

(назва роботи)

здобувача наукового ступеня доктора філософії

Регіда Павло Геннадійович

(прізвище, ім'я, по батькові)

з галузі знань 12 Інформаційні технології

(шифр, назва галузі знань)

за спеціальністю 123 Комп'ютерна інженерія

(шифр, назва спеціальності)

Публічна презентація проведена на кафедрі Комп'ютерної інженерії та інформаційних систем

(назва)

«07» травня 2025 року, протокол №20.

1. Актуальність теми дослідження. Використання інформаційних технологій (ІТ) для різних сфер у сучасному житті та практиці є розповсюдженим явищем, що дозволяє автоматизувати рутинні процеси. Таке активне використання супроводжується використанням програмного забезпечення (ПЗ) та різного рівня конфіденційності файлів користувача. Зважаючи на це, зловмисники вдаються до різних підходів для отримання даних, застосовуючи зловмисне програмне забезпечення (ЗПЗ) різних видів та класифікацій. Сучасні методи, хоч і забезпечують високий рівень їх виявлення, але потребують постійного розвитку. Це пов'язано із тим, що розробники ЗПЗ прикладають усіх зусиль, щоб знайти вразливості в нових застосунках та в програмних оновленнях уже існуючих. Особливу увагу потрібно, також, приділити окремому випадку ЗПЗ – поліморфним вірусам, які наділені широким спектром методів уникнення виявлення для уникнення виявлення антивірусними програмними засобами (АПЗ). Враховуючи те, що такі методи реалізуються великою кількістю підходів, а їх різне комбінування потенційно може створювати велику кількість нових загроз для користувачів, то ПЗ, яке вони використовують та їх дані, є складним для дослідження та, відповідно, виявлення.

Ефективним та безпечним рішенням, що застосовується в більшості сучасних засобах виявлення та ідентифікації ЗПЗ є використання технології пісочниць. Основна перевага використання пісочниць пов'язана із використанням технологій емуляції та ізольованого середовища виконання, що надає безпечний та контрольований характер процесу аналізу. Таке рішення є провідним та потребує детального аналізу і дослідження з метою створення нових методів виявлення або удосконалення уже існуючих на їх основі.

Розробники ЗПЗ активно досліджують методи, якими відбувається їх виявлення і вдаються до різних стратегій їх захисту, зокрема застосовують

анти-емуляційні методи. Ці методи націлені на аналіз середовища виконання, з метою визначення присутності емуляції, що дозволяє приховувати аномальну поведінку на хості. Таким чином, автори ЗПЗ намагаються приховати його аномальну поведінку або відтермінувати його виявлення у часі. В разі виявлення, його сигнатура буде проаналізована та буде додана у відповідну базу усіх сучасних антивірусних програмних засобів (АПЗ) та більше не буде становити загрози. Тому, важливим завданням є організація дослідження динамічної емуляції для перевірки ПЗ на наявність аномальної поведінки. Використання такого підходу дозволить відтворювати ПЗ в різних умовах, які будуть забезпечуватись різними факторами емуляції. Аналізуючи результат відтворення дозволить зробити висновок про аномальність поведінки.

Особливістю використання емуляції є надлишкове використання обчислювальних ресурсів системи порівнюючи із звичним відтворенням програмних застосунків на хості. Застосування динамічного емулювання потребує застосункових обчислювальних ресурсів, тому буде необхідно залучати наукові дослідження суміжних галузей для ефективного її вирішення. Одним із передових та перспективних напрямків є залучення розподілених комп'ютерних систем для вирішення поставленої задачі, які можуть залучити обчислювальні ресурси різнорідних хостів.

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.

У дисертації вперше одержані такі нові наукові результати:

- 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;

- 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;

- 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;

- 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.

4. Теоретичне та практичне значення результатів дисертації

Розроблено централізовану грід-обчислювальну систему виявлення інфікованих програм, зокрема таких, що застосовують методи виявлення емуляції та обфускації коду. Система використовує автономні обчислювальні елементи для розподіленого виконання завдань, пов’язаних з аналізом інфікованих програм в ізольованому середовищі. Особливістю запропонованої централізованої розподіленої системи є використання засобів для аналізу інфікованих програм, що поєднують базові реалізації пісочниці та емулятора, які розгортаються на обчислювальних елементах системи. Для ефективного використання залучених обчислювальних ресурсів для аналізу інфікованих програм в модифікованих ізольованих середовищах, система використовує модифікований алгоритм розподілу завдань який враховує гетерогенність обчислювальних елементів. Крім того, з метою оптимізації залучених обчислювальних ресурсів використовується оцінювання довіри автономних обчислювальних елементів, що базується на рольовій моделі і при цьому зберігає необхідний рівень захисту обчислень. Синтезовані системи такого можуть бути використані іншими науковцями та розробниками для задач, що пов’язані із аналізом особливостей виконання зразків програм.

За результатами проведених експериментальних досліджень встановлено, що розроблена централізована грід-обчислювальна система забезпечує коректне функціонування в умовах динамічного середовища виконання, ефективне залучення акумульованих обчислювальних ресурсів для виконання задач виявлення інфікованих програм, а також гарантоване правильне виконання поставлених завдань.

Пояснення: дисертація повинна містити наукові положення, нові науково обґрунтовані теоретичні та/або експериментальні результати проведених досліджень, що мають істотне значення для певної галузі знань та підтверджуються документами, які засвідчують проведення таких досліджень, а також свідчити про особистий внесок здобувача в науку та характеризуватися єдністю змісту.

5. Використання результатів роботи

Результати дисертаційної роботи впроваджено у (Додаток Б):

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 спеціальностей 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»

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі Регіди П.Г.

Дисертаційна робота виконана на кафедрі комп'ютерної інженерії та інформаційних систем, Хмельницького національного університету,
(*назва кафедри (відділу), назва установи)*
науковий керівник д.т.н., професор, професор кафедри комп'ютерної інженерії та інформаційних систем Савенко О.С.
(*науковий ступінь, вчене звання, посада, прізвище, ініціали)*

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Регіди Павла Геннадійовича
(прізвище, ініціали здобувача)
є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 10 наукових праць. Основні результати дисертації викладені у: 4 статті у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б, одна з яких, згідно із п. 8 Постанови Кабінету Міністрів України від 12 січня 2022 р. №44, може бути зарахована як 0,5 публікації, оскільки число співавторів у ній (разом із здобувачем) становить більше двох осіб – **отже, для захисту зараховано 3,5 наукових публікацій з викладеними основними результатами досліджень.** Крім цього, результати дисертації викладені у 6 публікаціях, які засвідчують апробацію матеріалів дисертації (4 статті в матеріалах конференцій, що індексуються в наукометричній базі Scopus, 2 публікації в матеріалах міжнародних наукових конференцій) та 1 свідоцтво про реєстрацію авторського права на твір.

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Регіда П.Г., Бармак О.В., Каштальян А.С., Манзюк Е.А. Концепція застосування розподілених систем для аналізу поліморфних вірусів. *Вісник Хмельницького національного університету. Технічні науки.* 2024. Т. 331. №1. С. 38-43. DOI: https://doi.org/10.31891/2307-5732-2024-331-4

Регідою П.Г. проведено аналіз сучасних способів організації розподілених систем в контексті виявлення зловмисної поведінки в інфікованих програмах. Бармак О.В. визначив ключові характеристики для дослідження функціонування розподілених систем, а саме: стійкість та рівновага. Каштальян А.С. запропонована концепція розподіленої системи для виявлення інфікованих програм. Манзюк Е. запропонував планування експерименту та провів аналіз його результатів.

2. Регіда П.Г., Савенко О.С. Метод виявлення зловмисної активності в інфікованих програмах. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2024. №1. С. 178-186. DOI: https://doi.org/10.32782/IT/2024-4-21

Регідою П.Г. розроблено метод виявлення інфікованої програми із використанням грід-обчислювальної системи. Савенко О.С. запропонував оптимізацію аналізу пам'яті програми при формуванні поведінки інфікованої програми.

3. Регіда П.Г. Метод організації розподіленої системи виявлення інфікованих програм в ізольованих середовищах. Вісник Хмельницького національного університету. Технічні науки. 2025. Т. 347. № 1. С. 554-560. DOI: https://doi.org/10.31891/2307-5732-2025-347-76

4. Регіда П.Г. Поведінкова модель довіри в грід обчислювальній системі на основі нечіткої логіки. Вимірювальна та обчислювальна техніка в технологічних процесах. 2025. №1 (2025). С. 287-293. DOI: https://doi.org/10.31891/2219-9365-2025-81-35

Свідоцтво про реєстрацію авторського права на твір:

5. Авторське свідоцтво №134190. Україна. Комп'ютерна програма «Програмне забезпечення організації розподіленої системи виконання програмного коду в ізольованих середовищах» («РСВКІС»). Дата реєстрації: 10 березня 2025 р. / Регіда П. Г., Савенко О. С., Нічепорук А. О., Дрозд А. І.

Регідою П.Г. розроблено програмні частини центрального сервера та обчислювального елементу для розподіленого виявлення наявності зловмисної поведінки в інфікованих програмах. Савенко О.С. сумісно із Нічепоруком А.О. виконували адміністрування та концептуалізацію дослідження, розробку теоретичних засад для реалізації мережевого протоколу в розподіленій системі, рецензування та коригування рукопису. Дрозд А.І. сумісно із Регідою П.Г. займався розробкою настільних інтерфейсів програмних частин центрального сервера та обчислювального елементу, реалізацією мережевої взаємодії в системі та пошуком необхідних реалізованих бібліотек та фреймворків.

Праці, які засвідчують апробацію матеріалів дисертації:

6. Регіда П. Г. Засіб розподіленого виявлення зловмисного програмного забезпечення із використанням технології емулювання. *XX ювілейна міжнародна науково-практична конференція «Математичне та програмне забезпечення інтелектуальних систем» (МПЗІС-2022)*, Дніпро, Україна, листопад 23-25, 2022. С. 170-171.

7. Rehida P., Sochor T., Martynyuk V., Tarasova O., Orlenko V. A distributed malware detection model based on sandbox technology. *2023 4th International Workshop on Intelligent Information Technologies & Systems of Information*

Security (IntelITSIS), Khmelnytskyi, Ukraine, March 22–24, 2023. P. 475-485. *(Scopus)* URL: https://ceur-ws.org/Vol-3373/paper32.pdf

Регідою П.Г. розроблено модель для аналізу інфікованих програм на основі пісочниці. Сохор Т. запропонував алгоритм залучення нових обчислювальних елементів в систему. Мартинюк В запропонував алгоритм правильності виконання на основі голосування. Тарасова О. запропонувала використання довіреного обчислювального елементу для верифікації голосування. Орленко В. представила алгоритм залучення проміжних серверів.

8. Rehida P., Savenko O., Kashtalian A., Sachenko A. Malware Detection Tool Based on Emulator State Analysis. 2023 *IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Dortmund, Germany, 7–9 September 2023. P. 135-140. *(Scopus)* DOI: https://doi.org/10.1109/IDAACS58523.2023.10348678

Регідою П.Г. розроблено базовий засіб для формування поведінки виконання програми в ізольованому середовищі. Савенко О.С. запропонував концепцію для розроблення моделі комп'ютерних систем для аналізу інфікованих програм. Каштальян А. провела аналіз методів протидії емуляції та обфускації. Саченко А. запропонував дослідити часову залежність формування станів різними стратегіями;

9. Rehida P., Markowsky G., Sachenko A., Savenko O. State-based Sandbox Tool for Distributed Malware Detection with Avoid Techniques. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Athens, Greece, 13–15 October 2023. P. 1-6. *(Scopus)* DOI: https://doi.org/10.1109/DESSERT61349.2023.10416467

Регідою П. розроблено програмну частину обчислювального елементу розподіленої системи, який містить засіб для аналізу виконуваних програм. Марковський Дж. запропонував дослідити зміну поведінки для порівняння оригінальної і обфускованої програм. Саченко А. запропоновано експеримент дослідження ефективності застосування розподіленої системи для аналізу програм. Савенко О. визначив стратегії поведінки виконання інфікованих програм в цільовому середовищі.

10. Rehida P., Savenko O., Sachenko A., Drozd A., Vizhevski P. A trust model that ensures the correctness of computing in grid computing system. *2024 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS)*, Khmelnytskyi, Ukraine, March 28, 2024. P. 388-401. *(Scopus)* URL: https://ceur-ws.org/Vol-3675/paper28.pdf

Регідою П. розроблено модель із ролями обчислювальних елементів розподіленої системи. Савенко О. запропонував визначення ролі обчислювального елемента на основі його поведінки під час функціонування системи. Саченко А. запропонував використання рейтингу обчислювального елементу та бінарного класифікатора для його коригування. Дрозд А. провів аналіз готових засобів для розгортання бінарного класифікатора. Віжевський П. сформував список інформації який можна збирати на обчислювальному елементі.

11. Регіда П., Капустян М. Лигун О. Динамічне емулювання як засіб виявлення поліморфних вірусів із маскувальними техніками. *The 13th International Scientific Conference «ITSec»*, м. Львів, Україна Травень 9-11, 2024. С. 179-180.

International Scientific Conference «ITSec», м. Львів, Україна Травень 9-11, 2024. С. 179-180.

Регідою П. запропоновано концепцію використання модифікованих ізольованих середовищ для виявлення зловмисного прояву. Капустян М. представила базову модель інфікованої програми. Лигун О. представив спосіб формування модифікованого ізольованого середовища.

ВВАЖАТИ, що дисертаційна робота Регіди Павла Геннадійовича

(прізвище, ініціали здобувача)

«Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання»,

(назва)

яка 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, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 123 – Комп'ютерна інженерія

(шифр, назва)

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Методи та засоби організації розподілених систем виявлення інфікованих виконуваних програм, стійких до емуляції в середовищі виконання»

назва роботи

подану Регідою Павлом Геннадійовичем

прізвище, ім'я, по батькові

на здобуття ступеня доктора філософії, до захисту.

Головуючий публічної презентації
(завідувач кафедри):

д.т.н., доцент
(науковий ступінь,

вчене звання, посада)

Підпис дійсний *підпис*
Засвідчую
Начальник відділу кадрів
І.С.Мартинюк

Ольга ПАВЛОВА.
Ім'я ПРІЗВИЩЕ