Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії ___Регіда Павло Геннадійович_____,
(власне ім'я, прізвище здобувача (ки))

__1991_ року народження, громадянин (ка) _____України_____,
(назва держави, громадянином якої є здобувач (ка))

освіта вища: закінчив (ла) у __2015__ році _____КПІ ім. Ігоря Сікорського_____
(найменування закладу вищої освіти)

за спеціальністю (спеціальностями) _____Комп'ютерні системи та мережі_____,
(за дипломом)

працює старшим викладачем кафедри комп'ютерної інженерії та інформаційних систем
(посада)

в Хмельницькому національному університеті Міністерства освіти і науки України,
(місце основної роботи, підпорядкування, місто)

м. Хмельницький

виконав (ла) акредитовану освітньо-наукову програму «Комп'ютерна інженерія» Хмельницького національного університету

Разова спеціалізована вчена рада, утворена наказом Хмельницького національного університету
(повне найменування закладу вищої освіти

Міністерства освіти і науки України, м. Хмельницький від «_16_» _травня__ 2025 року № 41-ас
(наукової установи), підпорядкування (у родовому відмінку), місто)

у складі:

Голови разової
спеціалізованої вченої ради – Тетяни ГОВОРУЩЕНКО, доктора технічних наук, професора, декана факультету інформаційних технологій Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Рецензентів - Сергія ЛИСЕНКА, доктора технічних наук, професора, професора кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Юрія КЛЬОЦА, кандидата технічних наук, доцента, завідувача кафедри кібербезпеки Хмельницького національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

Офіційних опонентів - Андрія КОВАЛЕНКА, доктора технічних наук, професора, завідувача кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки.
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)
Наталії ВОЗНОЇ, доктора технічних наук, професора, професора кафедри спеціалізованих комп'ютерних систем Західноукраїнського національного університету
(власне ім'я, прізвище, науковий ступінь, вчене звання, посада, місце роботи)

на засіданні «3» липня 2025 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 – Інформаційні технології
(галузь знань)

_____Павлу РЕГІДІ_____
(власне ім'я, прізвище здобувача (ки) у давальному відмінку)

на підставі публічного захисту дисертації «МЕТОДИ ТА ЗАСОБИ ОРГАНІЗАЦІЇ РОЗПОДІЛЕНИХ СИСТЕМ ВИЯВЛЕННЯ ІНФІКОВАНИХ ВИКОНУВАНИХ ПРОГРАМ,

СТІЙКИХ ДО ЕМУЛЯЦІЇ В СЕРЕДОВИЩІ ВИКОНАННЯ»

(назва дисертації)

за спеціальністю (спеціальностями) 123 – Комп'ютерна інженерія

(код і найменування спеціальності (спеціальностей)

.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Дисертацію виконано у (в) Хмельницькому національному університеті Міністерства освіти і

(повне найменування закладу вищої освіти

науки України, м. Хмельницький

(найменування закладу вищої освіти (наукової установи), підпорядкування, місто)

Науковий керівник (керівники) Олег САВЕНКО, доктор технічних наук, професор,

(власне ім'я, прізвище, науковий ступінь,

професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету

(вчене звання, місце роботи, посада)

Дисертацію подано у вигляді спеціально підготовленого рукопису. Дисертація містить чотири нові науково обґрунтовані результати проведених здобувачем досліджень, які виконують конкретне наукове завдання організації розподілених систем обчислень для виявлення інфікованих програм на основі використання модифікованих ізольованих середовищ, що має істотне значення для галузі знань 12 – Інформаційні технології. Дисертація виконана державною мовою. Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації». Загальний обсяг дисертаційної роботи становить 188 сторінок друкованого тексту, з них 128 сторінок основного тексту, що відповідає встановленим освітньо-науковою програмою «Комп'ютерна інженерія» Хмельницького національного університету максимальному та мінімальному обсягам основного тексту дисертації.

Здобувач має 10 наукових публікацій за темою дисертації, з них 4 статті у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б:

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. (https://doi.org/10.31891/2307-5732-2024-331-4)
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. (https://doi.org/10.32782/IT/2024-4-21)
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. (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. С. 287-293. (https://doi.org/10.31891/2219-9365-2025-81-35)

У дискусії взяли участь (голова, рецензенти, офіційні опоненти, інші присутні) та висловили зауваження:

Говорущенко Тетяна Олександрівна, д.т.н., професор, декан факультету інформаційних технологій Хмельницького національного університету; Лисенко Сергій Миколайович, д.т.н., професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету; Кльоц Юрій Павлович, к.т.н, доцент, завідувач кафедри кібербезпеки Хмельницького національного університету; Коваленко Андрій Анатолійович, д.т.н., професор, завідувач кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки; Возна Наталія Ярославівна, д.т.н., професор, професор кафедри спеціалізованих комп'ютерних систем Західноукраїнського національного університету.

Зауваження:

Лисенко Сергій Миколайович, д.т.н., професор, професор кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету:

1) у першому розділі дисертаційної роботи не було зроблено акценту саме на ті системи, які використовують концепцію розподілених обчислень як засіб виявлення зловмисного програмного забезпечення;

2) в роботі рисунок 2.1 який визначений як «Модель інфікованої програми» окрім самих складових частин інфікованої програми також визначає вплив визначеної моделі на операційну систему та її складові частини. Тому вказана назва рисунку не відповідає поданому зображенню;

3) запропонований алгоритм розподілу задач базується на визначеному коефіцієнту складності виконання кожної інфікованої програми для оптимального розподілу навантаження на обчислювальні елементи. Для такої оцінки здобувач пропонує використовувати довірений обчислювальний елемент, але в явному вигляді такий елемент не фігурує на рисунку системи, а сама оцінка явно не представлена як крок запропонованого методу функціонування;

4) в роботі запропоновано використовувати рольову модель для визначення довіри кожного обчислювального елементу, але на рисунку 4.5, який демонструє налаштування розподілених обчислень в контексті рейтингу довіри, визначено параметр «Допустимий рівень», тому не зовсім ясно як це значення відноситься до запропонованих ролей, та як за допомогою представленого інтерфейсу адміністратор може керувати запропонованими рівнями довіри;

5) До одного з представлених експериментів в розділі 4 було додано 2 таблиці (Таблиця 4.5 та 4.6) із результатами аналізу поведінки виконання моделей інфікованих програм в модифікованих середовищах виконання. Ймовірно, таблиці демонструють результати проміжного аналізу визначених у формулою 3.13. Так як запропонований метод грунтується на результатах обох таблиць для визначення наявності зловмисної поведінки, здобувачу варто було б об'єднати таблиці в одну, та подати її в розширеному вигляді в додатках;

6) у дисертаційній роботі часто використовуються терміни «підзадачі» та «підзавдання», здобувачу варто було б узгодити термінологію з цього приводу. Окрім цього, зустрічаються деякі граматичні та стилістичні помилки, зокрема на сторінках 64, 66, 85, 104;

Кльоц Юрій Павлович, к.т.н, доцент, завідувач кафедри кібербезпеки Хмельницького національного університету:

1) у роботі недостатньо уваги приділено саме грід-системам як окремому типу розподілених обчислювальних систем;

2) в запропонованому методі організації обчислень варто було б врахувати транспортні часові витрати на передачу завдання від центрального сервера до обчислювального елементу, враховуючи тип розподіленої системи запропонований для вирішення поставленої задачі;

3) в експериментах, які визначають ефективність функціонування розробленої розподіленої обчислювальної системи у порівнянні із іншими подібними системами не було проведено порівняння саме ефективності виявлення інфікованих програм;

4) у запропонованому методі оцінювання довіри здобувач використовує вагові коефіцієнти для двох наборів параметрів, що характеризують поведінкові особливості обчислювальних елементів. Однак не уточнюється методика визначення цих коефіцієнтів;

5) на сторінці 17 визначено поведінку зловмисного програмного забезпечення як «аномальна(зловмисна?)» і потребує уточнення. Також, на сторінці 74 в реченні про стратегію виконання використано слово «очікуванні» два рази. Окрім цього, в роботі присутні деякі орфографічні та стилістичні помилки, а саме на сторінках 66, 93, 94.;

Коваленко Андрій Анатолійович, д.т.н., професор, завідувач кафедри електронних обчислювальних машин Харківського національного університету радіоелектроніки:

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;

Возна Наталія Ярославівна, д.т.н., професор, професор кафедри спеціалізованих комп'ютерних систем Західноукраїнського національного університету:

1) у першому розділі дисертаційної роботи не було повною мірою розглянуто основні підходи до виявлення поліморфних вірусів у складі проаналізованих програмних антивірусних застосунків і систем;

2) 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;

3) 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;

4) 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;

5) 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;

6) 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.

Результати відкритого голосування:

«За» ___5___ членів ради,

«Проти» ___0___ членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує

_____Павлу РЕГІДІ_____

(власне ім'я, прізвище, здобувача (ки) у давальному відмінку)

ступінь/ступеня доктора філософії з галузі знань _____12 – Інформаційні технології_____

(галузь знань)

за спеціальністю (спеціальностями) __123 – Комп'ютерна інженерія_____

(код і найменування спеціальності (спеціальностей)

_____.

відповідно до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти)

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої вченої ради _____ Тетяна ГОВОРУЩЕНКО

(підпис) (власне ім'я та прізвище)

М.П.