Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U001806

Особливі позначки: відкрита

Дата реєстрації: 20-05-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Регіда Павло Геннадійович

2. Pavlo Rehida

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 123

Назва наукової спеціальності: Комп’ютерна інженерія

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: Комп’ютерна інженерія

Дата захисту: 03-07-2025

Спеціальність за освітою: Комп'ютерні системи та мережі

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 9279

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 50.37.23, 50.41.27, 20.55

Тема дисертації:

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

2. Methods and tools for organizing distributed systems for detecting infected executable programs resistant to execution environment emulation

Реферат:

1. В дисертаційній роботі вирішується актуальна науково-прикладна з покращення ефективності функціонування грід-обчислювальних систем для виявлення інфікованих програм, що використовують методи уникнення від виявлення, за рахунок організації процесу розподіленого аналізу поведінки виконання із використанням програмних переривань на автономних обчислювальних елементах. Об'єктом дослідження є процес організації розподіленої системи для виявлення зловмисної поведінки в інфікованих програмах, які використовують методи уникнення виявлення. Предметом дослідження є методи організації розподілених систем із обчислювальними елементами, що мають рівень автономії для виявлення зловмисного прояву в інфікованих програмах. Метою дисертаційного дослідження є покращення ефективності функціонування грід-обчислювальних систем із автономними обчислювальними елементами для виявлення зловмисної передачі управління головним потоком в інфікованих програмах, що базується на концепції динамічного

стану емулювання середовища відтворення програмних засобів. Наукова новизна отриманих результатів 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. Практичне значення отриманих результатів полягає в розробці централізованої грід-обчислювальної системи виявлення інфікованих програм, зокрема таких, що застосовують методи виявлення емуляції та обфускації коду. 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. 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»

2. The dissertation solves a topical scientific and applied problem of improving the efficiency of grid computing systems for detecting infected programs that use detection evasion methods by organizing a process of distributed analysis of execution behaviour using program interrupts on autonomous computing elements. The object of the study is the process of organizing a distributed system for detecting malicious behaviour in infected programs that employ evasion techniques. The subject of research is methods for organizing distributed systems with computing elements that possess a level of autonomy for detecting malicious behaviour in infected programs. The aim of the dissertation research is to improve the efficiency of grid-computing systems with autonomous computing elements for detecting malicious control flow transfer in infected programs, based on the concept of dynamic emulation states of the program execution environment. The scientific novelty of the obtained results is as follows: 1) For the first time, a model of a centralized grid computing system has been developed, which considers the requirements for involving autonomous and heterogeneous computing elements to ensure task execution with correctness verification in a dynamic execution environment. This model enables the use of connected computing elements for analysing the execution behaviour of infected programs, supporting a distributed process of detecting malicious behaviour in infected programs; 2) A new method for synthesizing tools to generate behavioural patterns of infected programs has been developed. Unlike existing approaches, this method incorporates the use of a sandbox to execute the programs within a set of custom-modified isolated environments. Execution occurs via software interrupts and a basic emulator implementing a defined set of low-

level instructions. This enables the extraction of behavioural patterns from the state sets of emulated central processing units, facilitating the detection of malicious behaviour while accounting for the specific evasion techniques employed by malware developers; 3) The method for organizing the operation of grid computing systems has been improved. In contrast to existing methods, it utilizes a greedy algorithm to optimize workload distribution among autonomous heterogeneous computing elements and employs an additional active task queue. This ensures balanced execution of assigned tasks in distributed systems with dynamically changing topology, enhancing the distributed detection of malicious behaviour in infected programs; 4) The method for trust evaluation of autonomous computing elements has been improved. Unlike known methods, it introduces a role assignment mechanism based on elements of fuzzy logic. This allows for the optimization of computational resource usage by reducing redundant computations in systems operating within dynamic environments. The practical significance of the results obtained is development of a centralized grid computing system for detecting infected programs, including those employing anti-emulation and obfuscation techniques. Based on the results of experimental studies, it has been established that the developed centralized grid computing system ensures correct operation under dynamic execution environments, efficient utilization of accumulated computing resources for performing tasks related to the detection of infected programs. The theoretical and practical results of the research were implemented in ITT LLC (Khmelnytskyi), Nolt technologies LLC (Khmelnytskyi), as well as, in the educational process of the Khmelnytskyi National University when teaching disciplines at the Department of Computer Engineering and Information Systems for the specialty 123 Computer Engineering, in particular in the courses “Theory and Design of Computer and Cyber-Physical Systems and Networks”, “Security and Protection of Computer Systems”, “Computer Networks, System Administration and Cyber Security”

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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 (IntellTSIS), Khmelnytskyi, Ukraine, March 28, 2024. P. 388-401.
- 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.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U109936 0124U000980

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Савенко Олег Станіславович
2. Oleg S. Savenko

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Коваленко Андрій Анатолійович
2. Andriy A. Kovalenko

Кваліфікація: д.т.н., професор, 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, буд. 14, Харків, Харківський р-н., 61166, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Возна Наталія Ярославівна

2. Nataliia Y. Vozna

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, буд. 11, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Лисенко Сергій Миколайович

2. Sergii M. Lysenko

Кваліфікація: д.т.н., професор, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Кльоц Юрій Павлович

2. Yuriy P. Klyots

Кваліфікація: к.т.н., доц., 05.13.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Хмельницький національний університет

Код за ЄДРПОУ: 02071234

Місцезнаходження: вул. Інститутська, буд. 11, Хмельницький, Хмельницький р-н., 29016, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Говорущенко Тетяна Олександрівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Говорущенко Тетяна Олександрівна
Відповідальний за підготовку облікових документів	Синюк Олег Миколайович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна