Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U001846

Особливі позначки: відкрита

Дата реєстрації: 21-05-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Чайковський Максим Юрійович

2. Maksym Chaikovskyi

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'ютерні 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 9271

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 виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи

2. Methods and means of detection polymorphic viruses using a hybrid multi-agent system

Реферат:

1. Пошук та знешкодження комп'ютерних вірусів з кожним роком стає все більш актуальною та складною проблемою, адже вони несуть загрозу безперешкодному функціонуванню комп'ютерних систем, які використовуються у все більш критичних сферах діяльності людства. Тому, розроблення нових методів та засобів знешкодження зловмисного програмного забезпечення (ЗПЗ) є одним із перспективних та пріоритетних завдань досліджень у сфері комп'ютерних наук. Незважаючи на постійне вдосконалення антивірусного програмного забезпечення, генерація та поширення ЗПЗ збільшується з року в рік. Одна з найсерйозніших проблем, з якою стикається розробники антивірусного програмного забезпечення (ПЗ) – це автоматична мутація коду зловмисної програми. Методи мутації та перестановки коду зловмисної програми називаються поліморфізмом. Поліморфні віруси неможливо ідентифікувати сигнатурним аналізом. Тому, для цього необхідно використовувати нові, удосконалені методи аналізу сучасного ЗПЗ, а також комплексне поєднання існуючих методів та підходів. Тому, системний підхід до аналізу, виявлення, класифікації, встановлення темпів поширення поліморфних вірусів, що лежать в основі гібридних мультиагентних систем

виявлення поліморфних вірусів, є досить актуальною науково-практичною задачею. Об'єкт дослідження – процес виявлення поліморфних вірусів у комп'ютерних системах. Предмет дослідження – моделі, методи і програмні засоби гібридних мультиагентних систем для виявлення поліморфних вірусів у комп'ютерних системах. Метою дисертаційного дослідження є підвищення ефективності виявлення поліморфних вірусів у комп'ютерних системах за допомогою гібридних мультиагентних систем. Наукова новизна одержаних результатів полягає в наступному: 1) вперше розроблено архітектуру гібридних мультиагентних систем виявлення поліморфних вірусів, яка каскадно делегуючи повноваження, здійснює аналіз середовища, встановлює темпи поширення, виявляє, класифікує поліморфні віруси та використовує різні стратегії прийняття рішення, враховуючи типи загроз, що дало змогу визначати та використовувати оптимальний комплекс методів для виявлення поліморфних вірусів, а також здійснювати класифікацію поліморфних вірусів за рівнями складності, що підвищує рівень ефективності обраних стратегій прийняття рішення; 2) розроблено новий метод виявлення поліморфних вірусів, який на відміну від існуючих, дозволяє не лише збільшити ефективність виявлення поліморфних вірусів, але й визначати ймовірність належності виявлених вірусів до класу поліморфних та передбачає трьохетапне комбіноване застосування, з якого, на першому етапі використовуються алгоритми пошуку рядка, на другому – інтелектуальний аналіз даних, аналіз в пісочниці, машинне навчання, метод розробки структурних функцій, на третьому - ймовірнісні логічні мережі, що дало змогу класифікувати виявлені загрози за рівнем ймовірності їх належності до поліморфних вірусів; 3) удосконалено метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра, який, на відміну від існуючих, дозволяє дослідити вплив кількості використаних методів виявлення поліморфних вірусів на темп їх поширення у коливальному процесі та дає змогу визначити, яку кількість методів виявлення поліморфних вірусів необхідно використати; 4) удосконалено метод класифікації поліморфних вірусів, який, на відміну від існуючих, дозволяє не лише класифікувати поліморфні віруси за рівнями складності їх будови, але й визначати ймовірність їх належності до нечітких термів на рівні низький, нижче середнього, середній, вище середнього, високий кожного рівня складності, що дало змогу підвищити рівень обгрунтованості та ефективність обраних стратегій. Практичне значення отриманих результатів. За результатами виконаних досліджень розроблено архітектуру гібридних мультиагентних систем виявлення поліморфних вірусів, здійснено реалізацію розроблених методів та гібридну мультиагентну систему, яка дає змогу визначати та використовувати оптимальний комплекс методів для виявлення поліморфних вірусів, а також здійснювати класифікацію поліморфних вірусів за рівнями складності, що підвищує рівень ефективності обраних стратегій прийняття рішення. В результаті проведених експериментальних досліджень з гібридною мультиагентною системою, в основу функціонування якої покладено розроблений підхід, отримано наступні результати: при роботі з поліморфними вірусами першого рівня складності ефективність гібридної мультиагентної системи становить 98,87 %; при роботі з поліморфними вірусами першого і другого рівнів складності – 98,15 %; перших трьох рівнів складності – 97,45 %, перших чотирьох – 96,34 %, перших п'яти – 95,94 % та підтверджують ефективність запропонованого рішення.

2. The search and neutralization of computer viruses is becoming an increasingly urgent and complex problem every year, as they pose a threat to the smooth functioning of computer systems used in increasingly critical areas of human activity. Therefore, the development of new methods and means of neutralizing malicious software (MWS) is one of the promising and priority research tasks in the field of computer science. Despite the constant improvement of antivirus software, the generation and spread of MWS is increasing from year to year. One of the most serious problems faced by developers of antivirus software (SW) is the automatic mutation of the malicious program code. The methods of mutation and permutation of the malicious program code are called polymorphism. Polymorphic viruses cannot be identified by signature analysis. Therefore, for this it is necessary to use new, improved methods of analyzing modern MWS, as well as a complex combination of existing methods and approaches. Therefore, a systematic approach to the analysis, detection, classification, and establishment of the rates of spread of polymorphic viruses, which underlie hybrid multiagent systems for detecting polymorphic viruses, is a rather urgent scientific and practical task. The object of the study is the process of detecting

polymorphic viruses in computer systems. The subject of the study is models, methods, and software tools of hybrid multiagent systems for detecting polymorphic viruses in computer systems. The purpose of the dissertation research is to increase the efficiency of detecting polymorphic viruses in computer systems using hybrid multiagent systems. The scientific novelty of the results obtained is as follows: 1) for the first time, an architecture of hybrid multi-agent systems for detecting polymorphic viruses was developed, which, by cascading delegation of authority, analyzes the environment, determines the rate of spread, detects, classifies polymorphic viruses, and uses various decision-making strategies, taking into account the types of threats, which made it possible to determine and use the optimal set of methods for detecting polymorphic viruses, as well as to classify polymorphic viruses by levels of complexity, which increases the level of effectiveness of the selected decision-making strategies; 2) a new method for detecting polymorphic viruses has been developed, which, unlike existing ones, allows not only to increase the efficiency of detecting polymorphic viruses, but also to determine the probability of belonging of detected viruses to the class of polymorphic ones and provides for a three-stage combined application, of which, at the first stage, string search algorithms are used, at the second - intelligent data analysis, sandbox analysis, machine learning, a method for developing structural functions, at the third - probabilistic logical networks, which made it possible to classify detected threats according to the level of probability of their belonging to polymorphic viruses; 3) a method for determining the rate of spread of polymorphic viruses has been improved based on the use of the Lotka-Volterra model, which, unlike existing ones, allows investigating the influence of the number of used methods for detecting polymorphic viruses on the rate of their spread in an oscillatory process and allows determining the number of methods for detecting polymorphic viruses that need to be used; 4) the method for classifying polymorphic viruses has been improved, which, unlike existing ones, allows not only to classify polymorphic viruses by the levels of complexity of their structure, but also to determine the probability of their belonging to fuzzy terms at the levels of low, below average, average, above average, high for each level of complexity, which made it possible to increase the level of validity and effectiveness of the selected strategies. Practical significance of the results obtained. Based on the results of the research, the architecture of hybrid multiagent systems for detecting polymorphic viruses was developed, the developed methods were implemented, and a hybrid multiagent system was developed, which allows determining and using the optimal set of methods for detecting polymorphic viruses, as well as classifying polymorphic viruses by complexity levels, which increases the level of effectiveness of the selected decision-making strategies. As a result of experimental studies with a hybrid multiagent system, the functioning of which is based on the developed approach, the following results were obtained: when working with polymorphic viruses of the first level of complexity, the efficiency of the hybrid multiagent system is 98.87%; when working with polymorphic viruses of the first and second levels of complexity - 98.15%; the first three levels of complexity - 97.45%, the first four - 96.34%, the first five - 95.94%, and confirm the effectiveness of the proposed solution.

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:

- Чайковський М. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення. Measuring and Computing Devices in Technological Processes. 2024. № 2. С. 42-50.
- Савенко О., Чайковський М. Метод нечіткої класифікації зловмисного програмного забезпечення з використанням інтелектуального агента. Information Technology: Computer Science, Software Engineering and Cyber Security. 2024. № 3. С. 140-148.

- Чайковський М. Модель мультиагентної системи для виявлення поліморфних вірусів. Herald of Khmelnytskyi National University. Technical Sciences. 2024. № 347(1). С. 543-547
- Чайковський М. Архітектура та засоби мультиагентної системи виявлення поліморфних вірусів в комп'ютерних мережах. Measuring and Computing Devices in Technological Processes. 2025. № 1. С. 278–286.
- Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Comprehensive approach to the detection and analysis of polymorphic malware. CEUR Workshop Proceedings. 2024. Vol.3736. P.312-323. (Scopus)
- Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Modeling the detection process of polymorphic malware based on the Lotka-Volterra Model. CEUR Workshop Proceedings. 2025. Vol.3899. P. 244-253. (Scopus)

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 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 Олександр Володимирович
2. Alexandr V. Kovalenko

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Якименко Ігор Зіновійович

2. Ihor Yakymenko

Кваліфікація: к. т. н., доц., 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. Нічепорук Андрій Олександрович

2. Andrii O. Nicheporuk

Кваліфікація: к. т. н., доц., 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. Каштальян Антоніна Сергіївна
2. Kashtalian Antonina

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