

Голові разової спеціалізованої
вченої ради PhD 9271
Хмельницького національного університету
доктору технічних наук, професору
Тетяні ГОВОРУЩЕНКО

ВІДГУК

офіційного опонента на дисертаційну роботу

Чайковського Максима Юрійовича

на тему «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи», представлену на здобуття наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія

Актуальність теми дисертації. У сучасних умовах розвитку інформаційних технологій захист комп'ютерних систем і мереж набуває критичного значення. Постійне зростання обсягів даних, складність інформаційних інфраструктур та глобальна інтеграція мереж створюють сприятливе середовище для виникнення нових форм зловмисного програмного забезпечення. Особливу загрозу становлять поліморфні віруси, які змінюють свою структуру з кожною ітерацією, ускладнюючи їх виявлення традиційними антивірусними методами. Це породжує нагальну потребу в розробці нових, більш гнучких і адаптивних підходів до захисту комп'ютерних систем.

З позиції комп'ютерної інженерії, завдання виявлення поліморфних вірусів виходить за межі простого аналізу шкідливого коду. Воно вимагає поєднання високопродуктивних обчислювальних засобів, розподіленої обробки даних, адаптивних алгоритмів та інтелектуальних систем, здатних оперативно аналізувати поведінкові патерни, виявляти нові загрози та реагувати на них у реальному часі. Гібридні мультиагентні системи є перспективним рішенням, оскільки дозволяють розподілено і паралельно виконувати завдання аналізу, виявлення, класифікації та прийняття рішень у складному інформаційному середовищі.

Дослідження методів виявлення поліморфних вірусів на основі гібридної мультиагентної системи є актуальним напрямом у сфері комп'ютерних систем та мереж. Воно спрямоване на підвищення рівня інформаційної безпеки, забезпечення стійкості систем до новітніх кіберзагроз та оптимізацію використання ресурсів при виконанні захисних процедур. Актуальність теми також підсилюється зростаючою кількістю атак на критичні інфраструктури, що робить запропонований підхід важливим як у теоретичному, так і практичному вимірі комп'ютерної інженерії.

Все це підкреслює актуальність теми дисертаційної роботи Чайковського Максима Юрійовича, яка присвячена вирішенню наукової задачі створення мультиагентної системи для виявлення поліморфних вірусів.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету, а саме держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (№ держреєстрації 0124U000980), в якій автор дисертації був виконавцем.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни. Наукова новизна отриманих 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 обґрунтованості та ефективність обраних стратегій.

Наукові положення, висновки та рекомендації дисертаційної роботи Чайковського М.Ю. достатньо обґрунтовані коректним використанням математичного апарату, який лежить в основі розробленої гібридної мультиагентної системи виявлення поліморфних вірусів, підкріплені успішною реалізацією, ефективним практичним впровадженням результатів дисертаційного дослідження, яке підтвердило відповідність теоретичних досліджень з реальними результатами.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі, є достатньою і базується на детальному аналізі джерел за даною проблематикою, чіткій постановці задач дослідження, використанні сучасних методів дослідження, а також відображається у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів, які лягли в основу розробленої гібридної мультиагентної системи, підтверджується результатами експериментальних досліджень ефективної роботи мультиагентної системи.

Наукові положення, висновки та практичні рекомендації, сформульовані в дисертаційній роботі, є логічним наслідком отриманих результатів і ґрунтуються на послідовному та чіткому викладенні матеріалу. Отримані Чайковським М.Ю. висновки й запропоновані рішення можна вважати обґрунтованими та коректними. Це свідчить про повне виконання поставленого наукового завдання і належне опанування здобувачем методології наукових досліджень.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

Зазначена науково-прикладна задача відповідає предметній області Стандарту вищої освіти України зі спеціальності 123 Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти, зокрема, таким об'єктам вивчення та діяльності: методи та способи подання, отримання, зберігання, передавання, опрацювання та захисту інформації в комп'ютерних системах, архітектура та організація їх функціонування, інтерфейси та протоколи взаємодії їх компонентів.

Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям комп'ютерної інженерії.

Розглянувши результати перевірки дисертаційної роботи, можна зробити висновок, що дисертаційна робота Чайковського Максима Юрійовича є результатом самостійних досліджень здобувача та не містить елементів фальсифікації, фабрикації, компіляції, плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідне джерело.

Практичне значення одержаних результатів. 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.

У результаті проведених експериментальних досліджень з розробленою системою було підтверджене коректне функціонування гібридної мультиагентної системи, можливість застосування її до виявлення поліморфних вірусів.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «ІТТ» (м. Хмельницький), ПП «НОЛТ ТЕХНОЛОДЖИС» (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для спеціальності 123 Комп'ютерна інженерія.

Мова та стиль викладення результатів. Дисертаційна робота виконана українською мовою і вирізняється логічною побудовою, доступністю викладу та високим технічним рівнем. У тексті використано сучасну науково-технічну термінологію, а матеріал подано послідовно та зрозуміло для сприйняття. Стиль викладення відповідає нормам науково-технічної літератури. Дисертація добре структурована, а зміст належним чином ілюстровано таблицями та графічними матеріалами.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Повний обсяг роботи містить 211 сторінок друкованого тексту, з них анотація – на 11 стор., зміст – на 2 стор., основний текст – на 144 стор., список із

155 використаних джерел – на 17 стор., додатки – на 35 стор. Дисертація містить 35 рисунків та 36 таблиць.

Оприлюднення результатів дисертаційної роботи. За результатами проведених досліджень основні наукові результати опубліковано у 4 наукових статтях у трьох фахових наукових журналах України. Апробація засвідчена публікаціями 3 праць в матеріалах міжнародних та всеукраїнських конференцій, з яких 2 праці проіндексовані у наукометричній базі Scopus.

Наукові результати дисертаційної роботи доповідалися на таких конференціях: 1st International Workshop on Advanced Applied Information Technologies (AdvAIT-2024) (Khmelnyskyi, Ukraine - Zilina, Slovakia, December 5, 2024); XVI Всеукраїнська науково-практична конференція «Актуальні проблеми комп'ютерних наук АПКН-2024» (Хмельницький, Україна, 15-16 листопада 2024); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS-2024) (Khmelnyskyi, Ukraine, June 28, 2024).

Опубліковані праці відображають повноту викладу результатів дисертаційної роботи. Публікації характеризуються високим науковим рівнем, у яких дотримано принципів академічної доброчесності.

Отже, наукові результати, описані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

Недоліки та зауваження до дисертаційної роботи:

1. У п 1.3. автор здійснює аналіз існуючих мультиагентних систем виявлення зловмисного програмного забезпечення. Було б доцільно навести порівняльну таблицю з перевагами та недоліками проаналізованих систем у порівнянні із розробленою автором гібридною мультиагентною системою.

2. При здійсненні нечіткої класифікації поліморфних вірусів при використанні нечіткого логічного висновку автор для вхідних лінгвістичних змінних використовує трикутні функції належності (рис.3.11), а для вихідної – трапецієвидну (рис.3.12). Доцільною є більша деталізація обраних функцій належності.

3. У таблиці 3.12 відображена база правил для показника LPV (1 рівень складності поліморфних вірусів). Доцільно було б деталізувати базу правил і для

інших рівнів складності поліморфних вірусів.

4. На рисунку 4.3 відображено алгоритм роботи запропонованої автором гібридної мультиагентної системи. Доцільно була б більша його деталізація із врахуванням принципів роботи кожного інтелектуального агента системи.

5. При визначенні ефективності роботи гібридної мультиагентної системи в розділі 4 використовується метод експертного оцінювання для визначення вагових коефіцієнтів інтелектуальних агентів гібридної мультиагентної системи. Було б доцільно у додатках відобразити приклад анкети (форми), яку заповнювали експерти.

6. Рисунок 4.1 (с.129) «Мережа з гібридною МАС» вимагає більшої деталізації її складових.

Однак, зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

Висновок про дисертаційну роботу:

Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Чайковського Максима Юрійовича на тему «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є завершеним науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання, що має вагоме значення для галузі інформаційних технологій.

Дисертаційна робота 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 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024).

Здобувач Чайковський максим Юрійович заслуговує на присудження наукового ступеня доктора філософії в галузі знань 12 Інформаційні технології зі спеціальності 123 Комп'ютерна інженерія.

Офіційний опонент:

доцент кафедри кібербезпеки та
програмного забезпечення

Центральноукраїнського
національного технічного
університету,

доктор технічних наук, професор

Олександр КОВАЛЕНКО

Підпис доктора технічних наук, професора
Коваленко О.В. засвідчую"

Проректор з наукової роботи
та міжнародних зв'язків

Центральноукраїнського національного
технічного університету,
кандидат технічних наук, доцент



Андрій ТИХИЙ