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

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

1. Актуальність теми дослідження та її зв'язок із планами наукових робіт університету

Сучасний етап розвитку комп'ютерної інженерії характеризується високим рівнем автоматизації процесів, інтеграцією гетерогенних систем та активним впровадженням інтелектуальних технологій. У таких умовах значно зростає важливість забезпечення надійної кібербезпеки. Особливу загрозу становлять поліморфні віруси, здатні змінювати свою структуру з кожним зараженням, обходити засоби класичного виявлення і маскуватися під легітимні процеси. Це унеможливлює використання лише сигнатурних або евристичних методів, які втрачають ефективність у динамічному середовищі.

У зв'язку з цим постає необхідність створення інтелектуальних засобів аналізу й протидії таким загрозам, які здатні враховувати складність сучасного ландшафту атак. Актуальність теми визначається також тим, що стандартні антивірусні системи не забезпечують достатньо високого рівня адаптивності, гнучкості та масштабованості, необхідних для ефективного виявлення поліморфних вірусів у різних архітектурах комп'ютерних систем і мереж. Саме тому важливо впроваджувати системи, здатні до самонавчання, розподіленого аналізу та автономного ухвалення рішень.

Гібридна мультиагентна система, що поєднує кілька взаємодіючих інтелектуальних агентів, є перспективним напрямом для підвищення ефективності виявлення складних загроз. Такий підхід дозволяє розподіляти функціональність між агентами, забезпечуючи глибокий аналіз поведінки файлів, моделювання поширення, виявлення за різними критеріями, класифікацію та автоматизоване ухвалення рішень. Важливо, що мультиагентна архітектура дає змогу досягати високого рівня гнучкості, масштабованості, повторного використання компонентів, що є критично важливим у сфері комп’ютерної інженерії.

Таким чином, дослідження Чайковського М.Ю. спрямоване на розробку та обґрунтування методів і засобів виявлення поліморфних вірусів із використанням гібридної мультиагентної системи, має вагоме наукове і практичне значення. Це дозволяє не лише розширити існуючі підходи до протидії сучасним загрозам, а й сприяє підвищенню рівня захищеності комп’ютерних систем і мереж. У результаті, сформульоване дослідження цілком відповідає поточним викликам у сфері інформаційної безпеки та комп’ютерної інженерії.

Дослідження, результати яких наведено в дисертації, проведені в 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.

2. Формулювання наукової задачі, мети й задач дослідження

Здобувачем правильно визначено об’єкт і предмет дослідження. Так, об’єктом дослідження визначено процес виявлення поліморфних вірусів у комп’ютерних системах. Предметом дослідження встановлено моделі, методи і програмні засоби гібридних мультиагентних систем для виявлення поліморфних вірусів у комп’ютерних системах.

Мету дисертаційної роботи визначено, як підвищення ефективності виявлення поліморфних вірусів у комп’ютерних системах за допомогою гібридних мультиагентних систем.

Поставлену мету досягнуто в результаті розв'язання таких задач: 1) провести аналіз поліморфних вірусів за різними рівнями складності їх структури, методів та засобів їх виявлення за допомогою мультиагентних систем; 2) розробити моделі класів поліморфних вірусів згідно різних рівнів поліморфізму; 3) розробити архітектуру гібридних мультиагентних систем для виявлення, аналізу та класифікації поліморфних вірусів, а також модель інтелектуального агента в архітектурі гібридних мультиагентних систем для виявлення поліморфних вірусів; 4) удосконалити метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра для дослідження впливу кількості використаних методів виявлення поліморфних вірусів на темп їх поширення у коливальному процесі; 5) розробити метод виявлення поліморфних вірусів для покращення ефективності виявлення поліморфних вірусів та визначення ймовірності належності виявлених вірусів до класу поліморфних; 6) удосконалити метод класифікації поліморфних вірусів, який дозволить не лише класифікувати поліморфні віруси за рівнями складності їх будови, але й визначатиме ймовірність їх належності до нечітких термів кожного рівня складності; 7) розробити гібридну мультиагентну систему виявлення поліморфних вірусів, яка здійснюватиме аналіз середовища, встановлюватиме темпи поширення, виявлятиме, класифікуватиме поліморфні віруси та використовуватиме різні стратегії прийняття рішення і провести з нею експериментальні дослідження щодо встановлення ефективності функціонування та достовірності виявлення поліморфних вірусів і впровадити її у виробництво.

3. Наукова новизна одержаних автором результатів полягає у 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.

4. Аналіз основного змісту дисертації

У вступі обґрунтовано актуальність поставленої наукової проблеми, що полягає у створенні мультиагентної системи для виявлення поліморфних вірусів. Окреслено перспективність розробки гібридної мультиагентної системи, здатної реалізовувати функції аналізу середовища, оцінки темпів поширення загроз, виявлення, класифікації вірусів та прийняття обґрунтованих рішень щодо їх нейтралізації. Також встановлено зв’язок дослідження з актуальними науковими

напрямами, окреслено основні результати, практичне значення роботи та підприємства, де були впроваджені запропоновані рішення.

У першому розділі проаналізовано природу поліморфних вірусів, їхні типи та рівні складності. Проведено огляд сучасних методів виявлення та програмних засобів для діагностики комп'ютерних систем щодо поліморфних загроз. Розглянуто існуючі мультиагентні підходи до протидії зловмисному програмному забезпеченню. На основі виконаного аналізу визначено наукову задачу та сформульовано цілі дослідження.

У другому розділі побудовано моделі класів поліморфних вірусів з урахуванням особливостей їх структури та поведінки. Запропоновано підхід до нечіткої класифікації таких вірусів на основі методу нечіткого логічного висновку. Описано архітектуру гібридної мультиагентної системи та структуру інтелектуального агента, яка слугує базою для створення ефективних рішень з виявлення складних вірусних загроз.

У третьому розділі запропоновано метод виявлення поліморфних вірусів, що поєднує різні підходи (пошук рядків, інтелектуальний аналіз, пісочницю, машинне навчання, ймовірнісні логічні мережі) для підвищення точності виявлення та оцінювання ймовірності належності вірусів до конкретного класу. Удосконалено метод оцінки темпів поширення загроз із використанням моделі Лотки-Вольтерра, що дозволяє коригувати стратегії виявлення. Також покращено підхід до класифікації з урахуванням нечітких характеристик, що дозволяє точніше визначати складність вірусу та обирати відповідні дії.

У четвертому розділі реалізовано розроблену гібридну мультиагентну систему, запропоновано методику оцінювання її ефективності, описано експериментальне середовище, проведено оцінку ефективності та наведено висновки щодо досягнутих результатів.

У розділі висновків систематизовано здобуті наукові та практичні результати, що підтверджують ефективність запропонованих методів і засобів виявлення поліморфних вірусів у комп'ютерних системах.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій

Наукові положення, висновки і рекомендації дисертації обґрунтовані коректним та доцільним використанням математичного апарату, успішною реалізацією розробленої гібридної мультиагентної системи виявлення поліморфних вірусів, ефективним практичним впровадженням результатів дисертаційної роботи на підприємствах, що продемонструвало відповідність теоретичних досліджень із реальними результатами.

6. Практичне значення одержаних результатів

Розроблена архітектура гібридної мультиагентної системи для виявлення поліморфних вірусів, яка заснована на концепції інтелектуального агента і функціонує за принципом каскадної взаємодії та делегування повноважень. Система забезпечує поетапний аналіз середовища, визначення темпів поширення загроз, виявлення та класифікацію поліморфних вірусів із подальшим вибором відповідних стратегій прийняття рішень з урахуванням характеру загроз. Такий підхід дозволяє адаптивно підбирати ефективний набір методів виявлення та здійснювати класифікацію вірусів за рівнями складності, що сприяє підвищенню ефективності захисних заходів і створює підґрунтя для подальшої розробки систем нового покоління з покращеними характеристиками виявлення поліморфних вірусів.

Гібридну мультиагентну систему впроваджено у виробництво, а проведені експерименти відображають досить високий рівень її ефективності, який залежить від роботи мультиагентної системи з поліморфними вірусами різних рівнів складності. При роботі з поліморфними вірусами першого рівня складності ефективність гібридної мультиагентної системи становить 98,87 %, при роботі з поліморфними вірусами першого і другого рівня складності – 98,15 %, перших трьох рівнів складності – 97,45 %, перших чотирьох – 96,34 %, перших п’яти – 95,94 %. Ефективність гібридної МАС за часом виявлення та використанням ресурсу становить 96,245 %. Отримані значення ефективності відображають досягнення мети роботи.

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, зокрема в курсах «Теорія і проєктування комп'ютерних та кіберфізичних систем і мереж», «Теорія і технології проєктування спеціалізованих операційних систем», «Методи розв'язування наукових задач комп'ютерної інженерії».

7. Особистий внесок здобувача полягає у розробленні методу виявлення поліморфних вірусів; удосконаленні методу встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра; удосконаленні методу класифікації поліморфних вірусів; розробленні архітектури 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. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 4-х наукових статтях у фахових наукових журналах України. Апробація засвідчена публікаціями 3-х праць в матеріалах міжнародних та всеукраїнських конференцій, з яких 2-і праці індексовані у наукометричній базі Scopus. У роботах, що опубліковані у співавторстві, здобувачеві належать: удосконалено метод класифікації поліморфних вірусів, який дозволяє не лише класифікувати поліморфні віруси за рівнями складності їх будови, але й визначати ймовірність їх належності до нечітких термів кожного рівня складності; розроблено комплексний підхід до виявлення та аналізу поліморфних вірусів; удосконалено метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра.

8. Структура та обсяг дисертації

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.

9. Зауваження

1. У пункті 1.3 представлено аналіз мультиагентних систем виявлення зловмисного програмного забезпечення. Доцільно було б більше уваги звернути на розгляд існуючих гібридних мультиагентних систем та особливості їх функціонування.

2. У пункті 3.1 відображений метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра. Доцільно було б використати і певні модифікації моделі Лотки-Вольтерра.

3. У пункті 3.2. необхідно було б детальніше відобразити, чому саме запропоновано трьохетапний підхід із набором відповідних методів виявлення поліморфних вірусів.

4. У пункті 3.3. відображена реалізація методу класифікації поліморфних вірусів на основі нечіткого логічного висновку у середовищі Matlab. Але наведений приклад бази правил для показника LPV (1 рівень складності). Доцільно було б розширити і для інших рівнів складності.

5. У дисертаційній роботі зустрічаються деякі граматичні та стилістичні помилки, а також рис.4.1. Мережа з гібридною МАС (ст. 129) вимагає більшої конкретики.

Втім, зазначені зауваження суттєво не впливають на загальний, доволі високий, рівень проведеного дослідження.

10. Загальний висновок

Вважаю, що дисертаційна робота Чайковського Максима Юрійовича за темою «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв’язання актуальної науково-прикладної задачі системного підходу до аналізу, виявлення, класифікації, дослідження темпів

поширення поліморфних вірусів, що лежать в основі гібридної мультиагентної системи виявлення поліморфних вірусів.

Дисертаційна робота «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи», 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 (зі змінами, внесеними згідно з Постановами Кабінету Міністрів України № 341 від 21.03.2022, № 502 від 19.05.2023, № 507 від 03.05.2024), а її автор, Чайковський Максим Юрійович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент:
к.т.н., доцент, доцент кафедри
фізики та електротехніки
Хмельницького національного університету Антоніна КАШТАЛЬЯН

«Підпис Антоніни КАШТАЛЬЯН засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК