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

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

У контексті стрімкого зростання обчислювальних потужностей, масштабування цифрових систем і активного впровадження технологій Інтернету речей, хмарних обчислень і віртуалізації, питання забезпечення стійкості комп'ютерних систем і мереж до шкідливих впливів набуває особливої важливості. Особливо складним є захист від поліморфних вірусів — одного з найнебезпечніших класів шкідливого програмного забезпечення, які постійно модифікують власну структуру, уникаючи традиційного виявлення. Їхня здатність до маскування та швидкої адаптації до середовища роботи створює нові виклики для інженерії захисту інформаційних систем.

Комп'ютерна інженерія як галузь на стику апаратного та програмного забезпечення потребує нових архітектур безпеки, здатних не лише виявляти складні загрози, а й оперативно адаптуватися до їх змін. У зв'язку з цим мультиагентні системи, що поєднують у собі автономність, взаємодію, розподіленість і інтелектуальну обробку даних, виявляються перспективними в задачах виявлення шкідливих впливів. Їх використання дозволяє розподіляти

навантаження між різними рівнями аналізу, комбінувати кілька підходів до виявлення загроз та зменшувати час реакції системи при високому рівні точності.

Запропонована тематика дослідження спрямована на створення саме такої гнучкої й адаптивної гібридної мультиагентної системи, що враховує специфіку поліморфних вірусів і дозволяє реагувати на сучасні форми шкідливого ПЗ комплексно – на основі поведінкового аналізу, нечіткої класифікації, динамічного поширення загроз та прийняття рішень у реальному часі. Інтеграція таких інтелектуальних механізмів в архітектуру комп'ютерних систем дозволяє забезпечити новий рівень стійкості й надійності ІТ-інфраструктури.

Таким чином, дослідження Чайковського М.Ю., присвячене методам та засобам виявлення поліморфних вірусів із використанням гібридної мультиагентної системи, є не лише актуальним, але й стратегічно важливим для розвитку комп'ютерної інженерії. Воно забезпечує вагомий внесок у підвищення ефективності кіберзахисту, особливо в умовах швидкоплинних змін загрозливого середовища, що характерні для сучасних комп'ютерних систем і мереж.

Формулювання наукової задачі, мети й задач дослідження

Здобувачем коректно сформульовано об'єкт та предмет дослідження відповідно до висунутої гіпотези дослідження. 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.

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.

Короткий аналіз основного змісту дисертації

У вступі автором обґрунтовано актуальність теми, визначено мету, основні завдання, предмет та об’єкт дослідження, наведено наукову новизну, практичне значення одержаних результатів.

У першому розділі проаналізовано предметну область, поняття поліморфних вірусів та системи їх виявлення, проаналізовані методи виявлення поліморфних вірусів та мультиагентні системи виявлення зловмисного

програмного забезпечення. Також підведено підсумки проведеного аналізу та здійснено постановку задачі дослідження.

У другому розділі подано моделі класів поліморфних вірусів, розроблена архітектура гібридної мультиагентної системи виявлення поліморфних вірусів та модель інтелектуального агента в її структурі. Розроблена архітектура гібридної мультиагентної системи є основою для розроблення нових систем із підвищеною ефективністю виявлення поліморфних вірусів.

У третьому розділі наведено запропонований метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра; метод виявлення поліморфних вірусів на основі комплексного підходу; метод класифікації поліморфних вірусів на основі нечіткого логічного висновку.

У четвертому розділі автором запропоновано методику визначення ефективності функціонування гібридних мультиагентних систем виявлення поліморфних вірусів. Також, здійснено постановку і проведення експериментальних досліджень, оцінювання ефективності функціонування системи.

У висновках подано отримані наукові та практичні результати дослідження.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій

Наукові висновки та рекомендації, наведені в дисертації, ґрунтуються на адекватному та цілеспрямованому використанні математичних методів та алгоритмів, які лежать в основі розробленої архітектури гібридних мультиагентних систем виявлення поліморфних вірусів. Успішна реалізація розробленої системи, а також ефективне впровадження результатів дослідження на підприємствах демонструє відповідність отриманих теоретичних результатів реальним результатам їхнього використання.

Практичне значення одержаних результатів

Розроблено архітектуру гібридних мультиагентних систем виявлення поліморфних вірусів на основі інтелектуального агента, 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, а також є основою для розроблення нових систем із підвищеною ефективністю виявлення поліморфних вірусів. В структуру даної системи входять інтелектуальні агенти: «Аналіз», «Темп поширення», «Виявлення», «Класифікація», «Прийняття рішення», які виконують встановлені ролі та взаємодіють між собою. 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».

Особистий внесок здобувача

Розроблені та вдосконалені здобувачем методи, а саме метод виявлення поліморфних вірусів, метод встановлення темпу поширення поліморфних

вірусів, метод класифікації поліморфних вірусів, а також розроблена архітектура гібридних мультиагентних систем виявлення поліморфних вірусів забезпечують розв'язання поставлених у дисертації задач. Усі основні наукові та прикладні результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковані у 7 наукових працях, серед яких 4 статті у фахових наукових журналах України 3 публікації, які засвідчують апробацію матеріалів дисертації (2 статті в матеріалах конференцій, що індексуються в 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.

Апробація матеріалів дисертації

Наукові результати роботи доповідалися на таких конференціях: 1st International Workshop on Advanced Applied Information Technologies (AdvAIT-2024) (Khmelnytskyi, 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) (Khmelnytskyi, Ukraine, June 28, 2024).

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.

Зауваження

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації:

1. У дисертаційній роботі необхідно було б більше уваги акцентувати на найбільш важливих характеристиках та властивостях гібридних мультиагентних систем.

2. У розділі 2 автором відображена модель інтелектуального агента в структурі розробленої гібридної мультиагентної системи. Було б доцільно більше уваги приділити класифікації інтелектуальних агентів та відповідність інтелектуальних агентів «Аналіз», «Темп поширення», «Виявлення», «Класифікація», «Прийняття рішення» даній класифікації.

3. У роботі було б доцільно навести порівняння числового виміру ефективності розробленої гібридної системи виявлення поліморфних вірусів із іншими системами.

4. Було б доцільно деталізувати у додатках відображену у розділі 2 функцію винагороди (ст.83-84) для інтелектуальних агентів «Аналіз», «Темп поширення», «Виявлення», «Класифікація», «Прийняття рішення» при роботі гібридної мультиагентної системи.

5. Ст. 81 – некоректне використання термінології («цикл боротьби агента з вірусом»).

6. У дисертаційній роботі зустрічаються деякі граматичні та стилістичні помилки (таблиця 3.6 ст. 117, таблиця 3.10 ст.118).

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

Загальний висновок

Отже, дисертаційна робота Чайковського Максима Юрійовича за темою «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи» є завершеною науковою кваліфікаційною працею, яка містить новий та актуальний науково-прикладний внесок. Усі результати, які виносяться на захист є достовірними та отримані автором особисто.

Тому, з огляду на вищевказане, вважаю, що дисертаційна робота «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи», подану на здобуття наукового 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
комп'ютерної інженерії та
інформаційних систем
Хмельницького національного університету Андрій НІЧЕПОРУК

«Підпис Андрія НІЧЕПОРУКА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету Олег СИНЮК