

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

1. Актуальність теми дисертації

У сучасних комп'ютерних системах та мережах спостерігається стрімке зростання кількості складних та інтелектуально замаскованих кіберзагроз. Поліморфні віруси здатні змінювати власну структуру при кожному запуску або поширенні, становлять серйозний виклик для традиційних систем захисту. Використання стандартних сигнатурних методів дедалі частіше виявляється недостатнім, а отже, постає потреба у впровадженні нових рішень, які базуються на гнучких, адаптивних і розумних підходах до виявлення та реагування на загрози.

З погляду комп'ютерної інженерії, вирішення цього завдання вимагає застосування сучасних архітектур програмно-апаратних засобів, алгоритмів аналізу поведінки, а також систем штучного інтелекту, здатних працювати в умовах невизначеності та великих обсягів вхідних даних. Гібридні мультиагентні системи відкривають нові можливості у проектуванні ефективних засобів кіберзахисту, забезпечуючи автономну взаємодію спеціалізованих агентів, розподілену обробку даних та швидке прийняття рішень на основі комплексного аналізу.

Актуальність теми обумовлена необхідністю підвищення стійкості комп'ютерних систем до динамічних і складних загроз, зокрема таких, що мають здатність до самозміни. Розробка нових методів виявлення поліморфних вірусів з урахуванням обмежень у ресурсах, вимог до швидкості реагування та точності класифікації загроз є актуальним завданням у сфері захисту інформації, комп'ютерних мереж і систем, а також становить значний інтерес у контексті подальшого розвитку інтелектуальних кіберзахисних технологій.

Усе зазначене свідчить про важливість дослідження, проведеного Чайковським Максимом Юрійовичем, яке спрямоване на розв'язання наукової задачі розробки мультиагентної системи для виявлення поліморфних вірусів.

2. Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана 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.

3. Наукова новизна отриманих результатів

До основних наукових результатів дисертаційної роботи варто віднести:

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. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України.

Назва дисертації адекватно та повною мірою відображає її зміст.

У вступі обґрунтовано актуальність теми дисертації, визначено мету та основні завдання, предмет та об'єкт дослідження, відображено наукову новизну і практичне значення одержаних результатів.

У першому розділі проаналізовано поняття, типи поліморфних вірусів згідно рівнів складності, проаналізовані методи їх виявлення, програмні засоби діагностування комп'ютерних систем на наявність поліморфного зловмисного програмного забезпечення, проаналізовано існуючі мультиагентні системи виявлення зловмисного програмного забезпечення. Також, підведено підсумки проведеного аналізу та здійснено постановку задачі дослідження.

У другому розділі побудовано моделі класів поліморфних вірусів різних рівнів складності їх будови. Запропонована нечітка класифікація поліморфних вірусів за рівнями складності із використанням нечіткого логічного висновку. 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 розроблено метод виявлення поліморфних вірусів, який дозволяє не лише збільшити ефективність виявлення поліморфних вірусів, але й визначати ймовірність належності виявлених вірусів до класу поліморфних. Удосконалено метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра. 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 на рівні низький, нижче середнього, середній, вище середнього, високий кожного рівня складності, що дало змогу підвищити рівень обґрунтованості та ефективність обраних стратегій.

У четвертому розділі розроблено гібридну мультиагентну систему виявлення поліморфних вірусів, запропоновано методику визначення ефективності її функціонування, опис експериментального середовища, оцінювання ефективності функціонування системи, а також підведено підсумки з отриманих результатів.

У висновках представлено отримані наукові та практичні результати дослідження.

5. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, їх достовірність

Сформульовані у дисертації наукові положення, висновки та рекомендації є аргументованими і підкріплені успішною реалізацією розробленої гібридної мультиагентної системи для виявлення поліморфних вірусів, ефективним практичним впровадженням результатів дисертаційної роботи на підприємствах.

Обґрунтованість наукових положень та висновків дисертації ґрунтується на детальному аналізі джерел, чіткій постановці мети і задач дослідження, використанні сучасних методів дослідження.

Достовірність результатів дисертації підтверджується їх апробацією на міжнародних і всеукраїнських наукових конференціях, а також їх впровадженням.

6. Практичні результати роботи

У дисертації розроблено гібридну мультиагентну систему 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 %. Отримані значення ефективності відображають досягнення мети роботи.

Теоретичні та практичні результати дослідження впроваджені на 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. Оформлення дисертації, дотримання вимог академічної доброчесності та повнота викладу наукових положень та результатів в опублікованих працях

Дисертаційна робота має логічну структуру і складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та трьох додатків.

Повний обсяг роботи становить 211 сторінок друкованого тексту, поміж яких, основний текст – на 144 сторінках, список використаних джерел зі 155 найменувань – на 17 сторінках та три додатки – на 35 сторінках. Дисертація містить 35 рисунків та 36 таблиць. Оформлення дисертації відповідає необхідним вимогам. У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами досліджень опубліковано 4 статті у наукових фахових виданнях України, 3 тез доповідей у збірниках матеріалів конференцій, з яких 2 праці індексовані в наукометричній базі Scopus.

Усі сформовані наукові положення і результати дисертації повністю викладено в опублікованих працях.

8. Мова та стиль дисертаційної роботи

Текст дисертаційної роботи викладено в логічній послідовності. Матеріал дисертації достатньо проілюстрований схемами, рисунками, графіками й таблицями. Мова і стиль викладення змісту, оформлення дисертації відповідають вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

Зауваження та рекомендації до дисертації:

1. На рисунку 1.1 (с.23) відображена щорічна кількість атак ЗПЗ з 2015 по 2023 рік, також здійснено прогнозування даного показника (с.24) на 2024 та 2025 роки. Було б доцільно врахувати і статистичні дані за 2024 рік та здійснити

прогнозування на 2025 та 2026 рік, що дозволило б підвищити актуальність опрацьованих статистичних даних та отриманого прогнозу.

2. У таблиці 3.2 (ст. 31) здійснено порівняння антивірусних програм стосовно використання методів виявлення та можливостей аналізу темпів поширення та класифікації поліморфних вірусів, в якій використовуються рівні: «низький», «середній», «високий», але деталізоване пояснення даних рівнів у розрізі окремих показників відсутнє.

3. У таблиці 3.1 (ст. 91) при використанні моделі Лотки-Вольтерра сформована бальна шкала для вхідних параметрів та відображено показник β . Доцільно було приділити більшу увагу, чому саме такі значення β використано.

4. У п. 3.1. «Метод встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра» відображено результати 3-х експериментів для визначення оптимальної кількості методів виявлення поліморфних вірусів, які необхідно використати. На мою думку необхідно було б збільшити кількість проведених експериментів та відобразити їх результати у додатках.

5. Для розрахунку інтегрального показника ефективності гібридної МАС автором використано підхід, який передбачає розгляд його в адитивній та мультиплікативній формі (с.134-135) та визначення їх середнього значення при розрахунку показника ефективності. Доцільно було б більше уваги приділити перевагам саме даного підходу.

Зазначені зауваження істотно не впливають на зміст дисертаційної роботи та не знижують її наукову новизну та практичну цінність.

Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Чайковського Максима Юрійовича на тему «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи», що 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).

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:

декан факультету комп'ютерних
інформаційних технологій
Західноукраїнського
національного університету,
кандидат технічних наук, доцент



Ігор ЯКИМЕНКО