ВИСНОВОК

про наукову новизну, теоретичне та практичне значення результатів дисертації

на тему: «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи»

здобувача наукового ступеня доктора філософії

Чайковського Максима Юрійовича

з галузі знань 12 «Інформаційні технології»

за спеціальністю 123 «Комп'ютерна інженерія»

Публічна презентація проведена на розширеному засіданні кафедри комп'ютерної інженерії та інформаційних систем «06» травня 2025 року, протокол №19.

У результаті аналізу опрацювання теоретичних і практичних положень дисертаційної роботи, поданих до розгляду наукових публікацій за темою дисертації, результатів виконання здобувачем освітньо-наукової програми, а також за підсумками проведення фахового семінару визначено нвступне.

1. Актуальність теми дослідження. 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.

Разом з тим, існуючі підходи вимагають їх удосконалення у розрізі мінімізації недоліків запропонованих методів, а також необхідності врахування рівнів складності поліморфних вірусів, тобто удосконалення методу їх класифікації. Тому необхідним є системний підхід до аналізу, виявлення, класифікації, дослідження темпів поширення поліморфних вірусів, що лежать в основі гібридних мультиагентних систем виявлення поліморфних вірусів і є досить актуальною науково-практичною задачею.

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.

2. Зв'язок роботи з науковими програмами, планами, темами. Дослідження, результати яких викладено в дисертації, виконано під час виконання окремих розділів науково-дослідної роботи за держбюджетною темою Хмельницького національного університету «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (ДР № 0124U000980), у яких автор був виконавцем і розробляв та вдосконалював архітектури моделей глибокого навчання, які були застосовані у дисертаційному дослідженні.

3. Наукова новизна отриманих результатів**.** У дисертації вперше одержані такі нові наукові результати:

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. Теоретичне та практичне значення результатів дисертації.

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 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.

5. Використання результатів 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».

6. Особиста участь автора в одержанні наукових та практичних результатів, що викладені в дисертаційній роботі. Всі основні результати дисертаційного дослідження, які представлені до захисту, одержані автором особисто.

Основні положення дисертації, наукові результати, висновки, пропозиції та рекомендації, які виносяться на захист, опубліковані у фахових наукових виданнях згідно чинних вимог. З наукових праць, що виконані у співавторстві, у дисертації виконано ідеї та положення, запропоновані особисто автором.

Дисертаційна робота виконана на кафедрі комп’ютерної інженерії та інформаційних систем Хмельницького національного університету, науковий керівник доктор технічних наук, професор, професор кафедри комп’ютерної інженерії та інформаційних систем Савенко О.С.

Розглянувши звіт подібності щодо перевірки на плагіат, встановлено, що дисертаційна робота Чайковського Максима Юрійовича є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають посилання на відповідне джерело.

Дисертація характеризується єдністю змісту та відповідає вимогам щодо її оформлення. Стиль викладення в дисертації матеріалів дослідження є науковим і

забезпечує доступність її сприйняття. Дисертаційна робота відповідає обраній темі, розкриває її та підтверджує, що автором вирішено поставлені у роботі завдання.

7. Перелік публікацій за темою дисертації. Аналіз наукових публікацій, повноти опублікованих результатів дисертації та особистого внеску здобувача, засвідчив, що результати дослідження, які викладені у дисертаційній роботі, повною мірою відображають основні положення та висновки роботи, доповідались та обговорювались на науково-практичних конференціях.

За темою дисертації опубліковано 7 наукових праць, серед яких 4 наукові статті 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. Загальний обсяг публікацій становить 4,32 др. арк., з яких особисто здобувачеві належить 3,90 др. арк.

Список публікацій здобувача за темою дисертації:

Наукові праці, в яких опубліковані основні наукові результати дисертації

1. Чайковський М. Комплексний підхід до виявлення та аналізу поліморфного зловмисного програмного забезпечення. *Measuring and Computing Devices in Technological Processes.* 2024. № 2. С. 42-50. DOI: https://doi.org/10.31891/2219-9365-2024-78-5 *(0,8 умов. друк. арк.).*

2. 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. DOI: https://doi.org/10.32782/IT/2024-3-15. *(0,79 умов. друк. арк.; особистий внесок автора полягає в удосконаленні методу 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 - 0,7 умов. друк. арк.).*

3. Чайковський М. Модель мультиагентної системи для виявлення поліморфних вірусів. *Herald of Khmelnytskyi National University. Technical Sciences.*

2024. № 347(1). С. 543-547. DOI: https://doi.org/10.31891/2307-5732-2025-347-74. *(0,44 умов. друк. арк.).*

4. 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. DOI: https://doi.org/10.31891/2219-9365-2025-81-34. *(0,87 умов. друк. арк.).*

Праці, які засвідчують апробацію матеріалів дисертації

5. Chaikovskyi M., Chaikovska I., Sochor T., Martyniuk I., Lyhun O. Comprehensive approach to the detection and analysis of polymorphic malware. *CEUR Workshop Proceedings* (ISSN 1613-0073). 2024. Vol.3736. P.312-323. URL: https://ceur-ws.org/Vol-3736/paper23.pdf. *(0,77 умов. друк. арк.; особистий внесок автора полягає в розробленні комплексного підходу до виявлення та аналізу поліморфних вірусів - 0,6 умов. друк. арк.).* ***Індексується і реферується в міжнародних базах даних:*** *Scopus.*

6. 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* (ISSN 1613-0073). 2025. Vol.3899. P. 244-253. URL: https://ceur-ws.org/Vol-3899/paper22.pdf. *(0,61 умов. друк. арк.; особистий внесок автора полягає в удосконаленні методу встановлення темпу поширення поліморфних вірусів на основі використання моделі Лотки-Вольтерра - 0,45 умов. друк. арк.).* ***Індексується і реферується в міжнародних базах даних****: Scopus.*

7. Чайковський М.Ю. Прогнозування кількості атак зловмисного програмного забезпечення у світі. *Актуальні проблеми комп'ютерних наук АПКН-2024 : матеріали XVI всеукр. наук.-практ. конф., м. Хмельницький, 15-16 лист. 2024 р.* / Хмельницький національний університет. Хмельницький, 2024. С. 534-536. URL: https://kn.khmnu.edu.ua/wp-content/uploads/sites/18/apkn-2024-corpuspaper.pdf. *(0,025 умов. друк. арк.).*

ВВАЖАТИ,

що дисертаційна робота Чайковського Максима Юрійовича «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, та відповідає напрямку наукового дослідження освітньо-наукової програми Хмельницького національного університету зі спеціальності 123 – Комп'ютерна інженерія.

РЕКОМЕНДУВАТИ:

Дисертаційну роботу «Методи та засоби виявлення поліморфних вірусів за допомогою гібридної мультиагентної системи», подану Чайковським Максимом Юрійовичем на здобуття ступеня доктора філософії, до захисту.

Головуючий публічної презентації,
завідувач кафедри комп'ютерної
інженерії та інформаційних систем
Хмельницького національного університету,
доктор філософії, доцент Ольга ПАВЛОВА

Підпис дійсний
Засвідчую
Начальник відділу кадрів
І.С.Мартинюк