Голові разової спеціалізованої
вченої ради **PhD 12563**
Хмельницького національного
університету
доктору технічних наук,
професору Едуарду МАНЗЮКУ

РЕЦЕНЗІЯ

на дисертаційне дослідження Дрозда Андрія Ігоровича
за темою «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів», подане на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

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

Комп'ютерні атаки (КА) на корпоративні мережі (КМ) відбуваються безперервно та постійно еволюціонують, стаючи дедалі складнішими. Для протидії таким загрозам застосовується широкий спектр засобів і систем безпеки. Водночас ці рішення не є повністю прихованими. Інформація про них часто доступна з відкритих джерел або комерційних пропозицій розробників, що дозволяє зловмисникам вивчати їхню архітектуру та принципи роботи. З часом, у процесі експлуатації або дослідження, атакуючі здобувають глибше розуміння особливостей функціонування таких систем, що дає змогу обходити захисні механізми. У результаті ефективність захисту може суттєво знижуватися. Щоб мінімізувати ці ризики, розробники постійно вдосконалюють засоби безпеки, прагнучи забезпечити їхню непередбачуваність для зловмисників. Це означає, що під час здійснення КА, зловмисник не повинен мати змоги швидко визначити логіку роботи системи захисту. Таким чином, поряд із традиційними підходами до виявлення та нейтралізації КА, особливого значення набуває створення рішень із недетермінованою поведінкою, які здатні вводити зловмисника в оману, зберігаючи при цьому високу ефективність і стабільність у довготривалій перспективі.

Окрему роль у цій сфері відіграють обманні системи, а також різноманітні приманки та пастки. Вони імітують реальні ресурси мережі з метою виявлення КА і відволікання зловмисників. Однак через свою доступність такі засоби також можуть бути досліджені, тому потребують постійного вдосконалення. Перспективним напрямом є їх інтеграція в єдині комплекси, де виникає необхідність забезпечення узгодженого, але водночас непередбачуваного

функціонування всіх компонентів. Сучасні обманні технології частково відомі, що обумовлює потребу у створенні нових підходів, здатних ускладнити аналіз їхньої поведінки. Одним із перспективних рішень є використання популяційних алгоритмів, які дозволяють формувати послідовність дій системи таким чином, щоб вона залишалася складною для прогнозування. Такі алгоритми здатні не лише підтримувати ефективність виявлення КА, але й забезпечувати тривалу адаптацію до змін у середовищі.

Особливий інтерес становлять алгоритми, натхненні природними процесами, оскільки вони відтворюють адаптивну та гнучку поведінку. Наприклад, алгоритм молі й полум'я демонструє здатність уникати локальних оптимумів і поступово наближатися до глобального розв'язку. Проте більшість існуючих реалізацій орієнтовані на неперервні задачі, але в сфері комп'ютерної інженерії переважають дискретні варіанти вибору, що потребує додаткової адаптації алгоритмів.

Тому виникає потреба у створенні нової архітектури або модернізації існуючих обманних систем, які поєднували б ефективність реагування на загрози з високим рівнем невизначеності для зловмисників. Важливим напрямом досліджень є розробка методів оптимізації рішень у таких обманних системах із використанням популяційних алгоритмів, що дозволить підвищити рівень захисту КМ від сучасних КА.

Дисертаційне дослідження Дрозда А.І. виконувалось у рамках держбюджетної науково-дослідної теми №2Б-2024 «Система виявлення ЗПЗ та комп'ютерних атак в корпоративних мережах з використанням хибних об'єктів атак та пасток» (номер держреєстрації 0124U000980) та держбюджетної науково-дослідної теми №1Б-2026 «Система забезпечення стійкості до витоку конфіденційної інформації в корпоративних мережах в умовах впливів комп'ютерних атак» (номер держреєстрації 0126U002082), в яких він був виконавцем.

Формулювання наукової задачі, мети й задачі дослідження.

Здобувачем визначено об'єкт і предмет дослідження, відповідно до теми та висунутої гіпотези дослідження. Об'єктом дослідження визначено процес організації обманних систем з приманками і пастками для виявлення КА та зловмисного програмного забезпечення (ЗПЗ) в КМ. Предметом дослідження визначено методи організації обманних систем з приманками і пастками для виявлення КА та ЗПЗ в КМ.

В дисертації було визначено метою дослідження покращення протидії КА та ЗПЗ в КМ шляхом оптимізації кроків обманних систем з приманками і пастками за рахунок синтезу популяційних алгоритмів в центрах прийняття

рішень. Для досягнення мети дослідження було сформульовано Дроздом А.І. сім завдань, які були розв'язані і подані в дисертації.

Наукова новизна отриманих автором результатів полягає в наступному:

1) удосконалено архітектуру обманних систем з приманками і пастками, в якій на відміну від відомих варіантів архітектури, здійснено синтез популяційних алгоритмів, зокрема алгоритму молі і полум'я, для оптимізації формування послідовності наступних кроків при здійсненні КА та дій ЗПЗ, уникнення повного перебору варіантів, швидкої збіжності обраних кроків при триваючих впливах та зміни послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж, а також врахування потенційної спроможності зловмисників до здійснення двоцільових КА;

2) розроблено новий метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі обманних систем з приманками і пастками, який, на відміну від відомих, характеризується формуванням дискретного простору пошуку з координатним поданням об'єктів, синтезом спірального сліду на основі секторного оцінювання потенційних кроків і кутових характеристик, урахуванням часу як параметра зміни кроків та динамічним переміщенням молі й полум'я для уникнення передчасної збіжності до локальних оптимумів, що дало змогу розробляти обманні системи, які забезпечують довготривале й адаптивне функціонування у процесі протидії зловмисникам у корпоративних мережах за рахунок зміни кроків для опрацювання подій;

3) розроблено новий метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах, в якому на відміну від відомих, в архітектурі обманних систем синтезовано популяційні алгоритми, зокрема алгоритм молі і полум'я, для здійснення ними вибору наступних кроків для уникнення реалізації зловмисниками двоцільових атак, що дає змогу уникати повного перебору варіантів з можливих кроків, швидкої збіжності обраних кроків при триваючих впливах та зміну послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж та ускладнює дії за рахунок прийняття рішень на основі популяційних алгоритмів з можливістю самостійно блокувати або активувати сервери чи комп'ютерні станції, приманки чи пастки під час встановлення потенційно зловмисних впливів в корпоративних мережах;

4) розроблено новий метод виявлення атак відмови в обслуговуванні у мережах на основі статистичних показників, який на відміну від відомих, базується на обчисленні статистичних ознак мережного IP-трафіку при розбитті потоку пакетів на часові вікна, і встановлює динамічні зміни трафіку на рівні

всього аналізованого періоду, що дозволяє підвищити достовірність виявлення атак відмова в обслуговуванні.

Короткий аналіз основного змісту дисертації.

У вступі обґрунтовано актуальність задачі підвищення ефективності протидії зловмисним діям у КМ шляхом удосконалення архітектури та методів функціонування обманних систем з приманками і пастками (ОСПП). Визначено важливість ОСПП, у яких рішення формуються на основі популяційних алгоритмів. Подано зв'язок дослідження з науковими роботами у цій сфері, а також наведено основні результати та їх практичне впровадження.

У першому розділі проаналізовано предметну область, існуючі обманні системи, приманки, пастки та методи виявлення КА і ЗПЗ. Розглянуто типи популяційних алгоритмів і їхні особливості.

У другому розділі запропоновано удосконалену архітектуру ОСПП із використанням популяційних алгоритмів, зокрема алгоритму молі й полум'я, для оптимізації формування послідовності дій, адаптації до змін середовища та протидії двоцільовим КА без повного перебору варіантів.

У третьому розділі розроблено метод синтезу дискретного алгоритму молі й полум'я з урахуванням дискретного простору, часу та оцінювання кроків. Запропоновано метод організації функціонування ОСПП, що забезпечує автономний вибір дій, адаптацію до змін і ускладнення роботи зловмисників.

У четвертому розділі представлено метод виявлення КА типу відмова в обслуговуванні на основі аналізу трафіку, а також описано програмну реалізацію, проведені експерименти й оцінювання ефективності системи.

У висновках узагальнено отримані результати, а в додатках наведено публікації, матеріали впровадження та програмний код.

Обґрунтованість і достовірність наукових положень, висновків і рекомендацій. Наукові висновки та рекомендації, які подані в дисертації, обґрунтовані коректним використанням теорії абстрактної алгебри, теорії розподілених систем для визначення архітектури ОСПП в розподілених середовищах та деталізованого представлення їх основних елементів та компонентів, теорії множин і теорії графів, теорії розподілених систем, методів оптимізації для розроблення алгоритму дискретної оптимізації молі і полум'я успішною програмною реалізацією та ефективним практичним впровадженням результатів в організаціях, що експлуатують комп'ютерні системи, яке продемонструвало відповідність теоретичних досліджень з реальними результатами застосування.

Практичне значення отриманих результатів.

Розроблено ОСПП для виявлення КА і ЗПЗ у КМ, яка відрізняється використанням алгоритму дискретної оптимізації молі й полум'я для прийняття та коригування рішень, а також інтеграцією методу виявлення КА на основі аналізу їх статичних характеристик.

Поєднання популяційних алгоритмів з архітектурою ОСПП дало змогу формувати такі послідовності дій, що дезорієнтують зловмисників під час проведення двоцільових КА. У процесі інтеграції алгоритму молі й полум'я було адаптовано його етапи до задач дискретної оптимізації, що створює основу для подальшого застосування інших алгоритмів такого типу.

Експериментальні результати підтвердили, що розроблена ОСПП стабільно функціонує в умовах динамічних змін корпоративного середовища, ефективно використовує приманки й пастки для виявлення інфікованих програм і забезпечує обґрунтований вибір подальших дій.

Особистий внесок здобувача полягає в розробленні методів та засобів організації функціонування ОСПП на основі популяційних алгоритмів. Основні наукові результати дисертаційної роботи отримані здобувачем самостійно. За результатами проведених досліджень основні наукові результати опубліковано у 6 наукових статтях, з яких 5 у фахових наукових журналах України та одна стаття в міжнародному науковому журналі, що індексується в наукометричній базі Scopus. Апробація засвідчена публікаціями 5 праць в матеріалах міжнародних конференцій та семінарів, які проіндексовані у наукометричній базі Scopus. Опубліковано 1 свідоцтво про реєстрацію авторського права на твір (програму).

Апробація матеріалів дисертації.

Апробацію основних положень, ідей, висновків дисертаційної роботи здійснено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідалися на міжнародних науково-практичних конференціях та семінарах: 5th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, March 28, 2024); 6th International Workshop on Intelligent Information Technologies & Systems of Information Security (IntelITSIS, Khmelnytskyi, Ukraine, April 04, 2025,); 14th International Conference on Dependable Systems, Services and Technologies (IEEE, DeSSerT, Athens, Greece, October 11-13, 2024); 1st International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS, Khmelnytskyi, Ukraine, June 28, 2024); 2nd International Workshop on Intelligent & CyberPhysical Systems (ICyberPhyS, Khmelnytskyi, Ukraine, July 4, 2025).

Структура та обсяг дисертації.

Дисертаційна робота складається з анотації, змісту, переліку умовних скорочень, вступу, чотирьох розділів, висновку, списку використаних джерел та п'яти додатків. Повний обсяг роботи містить 267 сторінок друкованого тексту, з них анотація – на 12 с., зміст – на 2 с., перелік скорочень – на 1 с., основний текст – на 150 с., список із 181 використаних джерел – на 19 с., додатки – на 68 с. Дисертація містить 29 рисунків та 14 таблиць.

Зауваження.

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. В розділі 1 недостатньо деталізовано алгоритм молі і полум'я. Зокрема, відсутнє покрокове подання стандартного алгоритму молі і полум'я та його особливості в контексті неперервного та дискретного простору пошуку.

2. В дисертації не деталізовано типи приманок і пасток, мереж приманок. Їх поділ за типами впливає на результат.

3. Сектор розташування елементів множини (рис. 3.4, с. 123) подано в дисертації як єдиний варіант, тобто область, для розміщених в ньому розв'язків для вибору. Але таких варіантів може бути більше і можна було їх ввести та порівняти між собою.

4. В першому розділі при огляді літератури у вступі бракує достатнього порівняльного аналізу дискретних варіантів МФО.

5. В дисертації жодного аналізу статистичної значущості для підтвердження повідомленого покращення продуктивності не надано. Крім того, показники продуктивності зосереджуються в основному на результатах оптимізації, тоді як показники системного рівня, такі як затримка виявлення, адаптивність з часом або стійкість до навчання зловмисників, не аналізуються.

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

Загальний висновок.

Вважаю, що дисертаційна робота Дрозда Андрія Ігоровича за темою «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів» містить нові науково обґрунтовані теоретичні та експериментальні результати в галузі 12 Інформаційні технології, які в сукупності забезпечують розв'язання актуальної науково-прикладної задачі розроблення методів для підвищення ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення архітектури та методів функціонування обманних систем з приманками і пастками.

Дисертаційна робота «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів», 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, Дрозд Андрій Ігорович, заслуговує на присудження ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Рецензент,
кандидат фізико-математичних наук,
доцент, доцент кафедри комп'ютерної
інженерії та інформаційних систем
Хмельницького національного університету _____ Тетяна КИСІЛЬ

«Підпис Тетяни КИСІЛЬ засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК