Голові разової спеціалізованої
вченої ради PhD **12563**
Хмельницького національного університету
доктору технічних наук, професору
Едуарду МАНЗЮКУ
29016, м. Хмельницький,
вул. Інститутська, 11

ВІДГУК ОФІЦІЙНОГО ОПОНЕНТА

на дисертаційну роботу Дрозда Андрія Ігоровича
на тему: «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів», подану до захисту на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології
за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертаційної роботи.

Комп'ютерні атаки на корпоративні мережі є постійними та такими, що безперервно удосконалюються. Незважаючи на застосування сучасних засобів захисту, їх ефективність поступово знижується, оскільки зловмисники мають змогу досліджувати комерційні системи безпеки та адаптувати свої дії до їх особливостей. У результаті поведінка таких засобів стає передбачуваною, що спрощує їх обходження. Тому актуальним є створення підходів, які забезпечують не лише виявлення атак, а й формування недетермінованої, складної для аналізу поведінки систем захисту.

Перспективним напрямом досліджень є застосування обманних систем, приманок і пасток, які здійснюють імітування реальних об'єктів мережі. Водночас через доступність таких рішень вони також потребують постійного вдосконалення. Ефективним підходом є їх інтеграція в єдині комплекси обманних систем з приманками і пастками із централізованим керуванням та динамічною поведінкою. У цьому випадку важливим завданням є забезпечення недетермінованого функціонування як окремих компонентів, так і системи в цілому.

Для розв'язання цієї задачі доцільним є використання популяційних алгоритмів, які дозволяють формувати адаптивні та складні для прогнозування послідовності дій. Такі алгоритми забезпечують оптимізацію вибору наступних кроків і здатні уникати локальних оптимумів, що підвищує ефективність протидії атакам у довготривалій перспективі. Особливий інтерес становлять алгоритми, натхненні

природними процесами, зокрема алгоритм молі і полум'я, який характеризується здатністю до глобального пошуку рішень.

Водночас більшість існуючих реалізацій популяційних алгоритмів орієнтована на неперервний простір пошуку, тоді як задачі вибору дій у корпоративних мережах орієнтовані на дискретний простір пошуку. Це зумовлює необхідність адаптації таких алгоритмів, зокрема через розроблення дискретного простору пошуку, правил переходів та функцій оцінювання рішень.

Таким чином, виникає потреба у створенні або вдосконаленні архітектури обманних систем, у яких вибір і коригування дій будуть одночасно адекватними до змін мережного середовища та складними для аналізу зловмисниками. Це ускладнюється відсутністю універсальних алгоритмів, які б поєднували адаптивність, ефективність і недетермінованість.

Отже, актуальною науково-прикладною задачею є підвищення ефективності протидії комп'ютерним атакам і зловмисному програмному забезпеченню в корпоративних мережах шляхом оптимізації дій обманних систем з приманками і пастками на основі синтезу популяційних алгоритмів у підсистемах прийняття рішень. Зазначена задача відповідає спеціальності 123 «Комп'ютерна інженерія» та пов'язана з дослідженням архітектури комп'ютерних систем і мереж, а також методів захисту інформації в корпоративних мережах.

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

Під час виконання дисертації Дрозд Андрій був виконавцем 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).

3. Наукова новизна отриманих результатів.

До основних наукових результатів дисертаційної роботи варто віднести такі:

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 комп'ютерних атак 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 комп'ютерних атак;

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.

4. Короткий аналіз основного змісту дисертації

Науковий рівень викладення дисертації відповідає вимогам МОН України. Назва дисертації адекватно і в повній мірі відображає її зміст та відповідність спеціальності 123 «Комп'ютерна інженерія».

У вступі обґрунтовано актуальність задачі підвищення ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення обманних систем з приманками і пастками. Визначено важливість обманних систем із використанням популяційних алгоритмів, наведено основні результати та їх практичне застосування.

У першому розділі проаналізовано обманні системи, приманки й пастки, а також методи виявлення комп'ютерних атак і зловмисного ПЗ. Розглянуто популяційні алгоритми та їх особливості.

У другому розділі розроблено моделі двоцільових атак і запропоновано архітектуру обманних систем з приманками і пастками із

використанням алгоритму молі й полум'я для оптимізації вибору дій, уникнення повного перебору та врахування змін середовища.

У третьому розділі подано метод синтезу алгоритму дискретної оптимізації молі й полум'я, що забезпечує адаптивність і запобігає локальним оптимумам. Також запропоновано метод організації функціонування обманних систем із автономним вибором дій.

У четвертому розділі розроблено метод виявлення атак типу «відмова в обслуговуванні» на основі аналізу трафіку. Описано програмну реалізацію системи, експерименти та оцінку її ефективності.

У висновках подано отримані основні 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 підкріпленими практичною реалізацією обманної системи з приманками і пастками.

Наукова обґрунтованість положень і висновків дисертації забезпечена аналізом наукових джерел, чітким формулюванням завдань дослідження та використанням сучасних методологічних підходів.

Достовірність одержаних результатів підтверджена їх апробацією на міжнародних наукових конференціях та семінарах, а також практичним впровадженням.

6. Практичні результати роботи

Розроблено обманну систему з приманками і пастками, призначену для виявлення комп'ютерних атак та зловмисного програмного забезпечення в корпоративних мережах. Її ключовою особливістю є реалізація підсистеми прийняття рішень, у межах якої вибір наступних кроків та їх адаптивне коригування здійснюються із застосуванням алгоритму дискретної оптимізації молі і полум'я. Додатково, в компоненти системи інтегровано метод виявлення комп'ютерних атак, що базується на аналізі статистичних показників мережного трафіку, що підвищує достовірність і оперативність реагування на загрози.

Синтез популяційних алгоритмів в архітектурі обманних систем дозволив формувати такі послідовності дій, які є складними для прогнозування та аналізу з боку зловмисників, що підвищує ефективність їх дезорієнтації під час проведення атак. У процесі інтеграції алгоритму молі і полум'я було не лише адаптовано його до умов дискретного простору пошуку, а й деталізовано основні етапи функціонування, включаючи формування кроків, правила переходів і механізми оцінювання рішень. Отримані результати можуть бути використані як основа для подальшої адаптації інших популяційних алгоритмів, натхненних природними процесами, до задач забезпечення кібербезпеки.

Результати експериментальних досліджень підтвердили, що розроблена обманна система з приманками і пастками забезпечує стабільне та коректне функціонування в умовах динамічних змін середовища корпоративних мереж. Система ефективно залучає приманки і пастки для виявлення інфікованих компонентів, а також демонструє здатність адаптивно обирати наступні кроки функціонування, забезпечуючи підвищення загального рівня захисту мережі.

Теоретичні та практичні результати дослідження впроваджені в ТОВ «Nolt technologies» (м. Хмельницький), ТОВ «ІТТ» (м. Хмельницький), а також, в освітньому процесі Хмельницького національного університету при викладанні дисциплін на кафедрі комп'ютерної інженерії та інформаційних систем для здобувачів спеціальності F7 Комп'ютерна інженерія, зокрема в курсах «Безпека та захист комп'ютерних систем», «Моделювання та методи оптимізації в наукових та експериментальних дослідженнях», «Методології забезпечення якості, надійності, гарантоздатності та безпеки комп'ютерних систем та мереж» та в освітній процес у блоці військово-спеціальних дисциплін другої кафедри Другого навчально-наукового інституту Воєнної академії імені Євгенія Березняка, які використані при удосконалені навчально-лабораторного комплексу.

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 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 використаного джерела – на 19 с., додатки – на 68 с. Дисертація містить 29 рисунків та 14 таблиць. Оформлення дисертації відповідає вимогам.

У дисертації не виявлено текстових запозичень і використання наукових результатів інших науковців без посилань на відповідні джерела.

За результатами досліджень опубліковано 6 статей у наукових фахових виданнях (одна стаття в міжнародному журналі, яка індексована в наукометричній базі Scopus, квартиль – Q2), одне свідоцтво про реєстрацію авторського права на твір (програму), 5 праць матеріалів конференцій, які 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. Дисертація містить достатню кількість ілюстративного матеріалу – схем,

рисунків, графіків і таблиць. Мова викладу, стиль та оформлення роботи повністю відповідають установленим вимогам до наукових праць.

9. Зауваження та дискусійні положення щодо змісту дисертації

Зауваження та рекомендації до дисертації:

1. При поданні моделі функціонування обманних систем згідно з популяційними алгоритмами викладення матеріалу стосується лише застосування алгоритму молі і полум'я, а інші популяційні алгоритми не розглядаються.

2. Недавні дослідження демонструють, що поєднання алгоритмів оптимізації з моделями на основі навчання, такими як нейронні мережі, ансамблеві методи в інших інженерних областях, може значно підвищити адаптивність і надійність складних систем, а також працює як основа глибокого навчання. В дисертації ці питання не розглянуто.

3. Недостатньо чітко в дисертації роз'яснено відмінність розробленого варіанту алгоритму дискретного MFO від існуючих бінарних або дискретних варіантів MFO поза контекстом його використання в архітектурі обманних систем.

4. Обговорення кібератак подвійного призначення та розширеної багатоетапної моделі атаки є коректним, але його інтеграція в цикл оптимізації не повністю продемонстрована. Залишається незрозумілим, як зміни на етапах атаки динамічно впливають на змінні оптимізації або оцінку придатності.

5. Метрика відстані D (розділ 4), що використовується в алгоритмі міграції серверного вузла, сформована на основі RTT та кількості хопів, однак не обґрунтовано вибір вагових коефіцієнтів між цими складовими, а також не досліджено чутливість результату до зміни цих коефіцієнтів.

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

10. Висновки щодо дисертації в цілому

На основі викладеного вище вважаю, що дисертація Дрозда Андрія Ігоровича на тему «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів», 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), а її автор, Дрозд Андрій Ігорович, заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 123 Комп'ютерна інженерія.

Опонент,
доктор технічних наук, професор,
професор кафедри програмного
забезпечення систем ДВНЗ «Ужгородський
національний університет» _____ Оксана МУЛЕСА

Підпис проф. О. Мулеси
ЗАСВІДЧУЮ:
Вчений секретар ДВНЗ «Ужгородський
національний університет» _____ Олена МЕЛЬНИК