Голові разової спеціалізованої
вченої ради PhD 12563
Хмельницького національного
університету
доктору технічних наук,
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 на здобуття ступеня доктора філософії з галузі знань
12 Інформаційні технології за спеціальністю 123 Комп'ютерна інженерія

1. Актуальність теми дисертації.

Комп'ютерні атаки на корпоративні мережі є постійними та такими, що безперервно удосконалюються. Попри використання сучасних засобів захисту, їх ефективність знижується через те, що зловмисники мають доступ до інформації про ці системи та можуть досліджувати їхню поведінку. У результаті засоби захисту стають передбачуваними, що спрощує їх обходження. Тому актуальним є створення систем із непрогнозованою поведінкою, які ускладнюють аналіз і підвищують ефективність протидії атакам і зловмисному програмному забезпеченню.

Одним із перспективних напрямів є використання обманних систем, приманок і пасток, які імітують реальні ресурси та відволікають зловмисників. Оскільки такі рішення також є доступними для аналізу, виникає потреба в їх постійному вдосконаленні та інтеграції в єдині комплекси обманних систем з приманками і пастками із різними типами централізації. Важливим завданням є забезпечення їх недетермінованого функціонування та адаптивного керування приманками і пастками.

Перспективним підходом до вирішення цієї задачі є використання популяційних алгоритмів, які дозволяють формувати складні для прогнозування послідовності дій системи. Такі алгоритми забезпечують оптимізацію вибору наступних кроків і здатні уникати локальних оптимумів. Особливий інтерес становлять алгоритми, натхненні природними процесами, зокрема алгоритм молі і полум'я, який дозволяє здійснювати ефективний пошук рішень у глобальному просторі.

Водночас більшість реалізацій популяційних алгоритмів орієнтовані на неперервні простори пошуку, тоді як у корпоративних мережах вибір дій має дискретний характер. Це зумовлює необхідність їх адаптації до дискретного простору та розроблення відповідних моделей і методів.

Отже, виникає потреба у розробленні архітектури обманних систем, у яких вибір і коригування дій буде одночасно адекватним до змін середовища та складним для аналізу зловмисниками. Це ускладнюється відсутністю ефективних алгоритмів, що поєднують адаптивність і недетермінованість.

Таким чином, актуальною науково-прикладною задачею є підвищення ефективності протидії комп'ютерним атакам у корпоративних мережах шляхом оптимізації дій обманних систем з приманками і пастками на основі синтезу популяційних алгоритмів у підсистемах прийняття рішень. Зазначена задача відповідає предметній області спеціальності 123 «Комп'ютерна інженерія» та пов'язана з дослідженням архітектури комп'ютерних систем, мереж, методів обробки й захисту інформації, а також розробленням і впровадженням рішень для забезпечення безпеки IT-інфраструктур.

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

Дрозд Андрій виконував дисертаційне дослідження 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).

3. Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукова новизна результатів дисертаційного дослідження 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 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 комп'ютерних 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.

Наукові положення, висновки і рекомендації дисертаційної роботи Дрозда Андрія обґрунтовані коректним використанням математичного апарату, ефективним практичним впровадженням результатів дисертаційного дослідження, яке продемонструвало відповідність теоретичних досліджень із отриманими експериментальними результатами. При розв'язанні поставленої науково-прикладної задачі використовувались основні положення теорії абстрактної алгебри та теорії розподілених систем для визначення архітектури обманних систем з приманками і пастками в розподілених середовищах та деталізованого представлення їх основних елементів та компонентів, теорії множин і теорії графів для визначення компонентів обманних систем з приманками і пастками, а також процесу синтезу популяційних алгоритмів, зокрема алгоритму молі і полум'я, в

архітектуру обманних систем, теорії розподілених систем для організації функціонування обманних систем з приманками і пастками та їх компонентів для виявлення комп'ютерних атак і зловмисного програмного забезпечення, методи оптимізації для розроблення алгоритму дискретної оптимізації молі і полум'я.

Обґрунтованість наукових положень та висновків, сформульованих у дисертаційній роботі Дрозда Андрія, є достатньою і базується на детальному аналізі джерел за досліджуваною проблематикою, чіткій постановці задач дослідження, використання новітніх методів дослідження, правильним застосуванням математичного апарату при теоретичному подані наукових положень дисертації, а також проявляється у якісному та аргументованому формулюванні висновків.

Достовірність та обґрунтованість запропонованих методів і засобів підтверджується результатами експериментальних досліджень та коректним застосуванням методів, що були використані під час виконання роботи.

Наукові положення, висновки та рекомендації, які сформульовані в дисертації, логічно випливають із результатів, отриманих за допомогою чітких перетворень.

Отже, в дисертаційній роботі поставлене наукове завдання виконано повністю, а здобувач повною мірою оволодів методологією наукового дослідника.

4. Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

За своїм змістом дисертаційна робота здобувача Дрозда Андрія відповідає Стандарту вищої освіти зі спеціальності 123 - Комп'ютерна інженерія для третього (освітньо-наукового) рівня вищої освіти та освітньо-науковій програмі ХНУ «Комп'ютерна інженерія» за спеціальністю 123 Комп'ютерна інженерія. Дисертаційна робота є завершеною науковою працею і свідчить про наявність особистого внеску здобувача у науковий напрям предметної області з комп'ютерної інженерії.

Розглянувши дисертаційну роботу, можна зробити висновок, що вона є результатом самостійних досліджень здобувача і не містить елементів плагіату та запозичень. Використані результати і тексти інших авторів мають належні посилання на відповідне джерело.

5. Практичне значення одержаних результатів.

Результатом дисертаційної роботи є розроблена архітектура обманних систем з приманками і пастками для виявлення комп'ютерних атака та

зловмисного програмного забезпечення в корпоративних мережах, особливістю якої є прийняття в ній рішень щодо наступних кроків та їх коригування з використанням алгоритму дискретної оптимізації молі і полум'я, а також імплементацією в її компонентах методу виявлення комп'ютерних атак на основі аналізу їх статичних показників. Також розроблено прототип обманної системи, з якою було проведено експериментальні дослідження, що підтвердили відтворюваність наукових результатів дисертації.

Результати дисертаційної роботи впроваджені в ТОВ Nolt technologies, ТОВ «ІТТ» (м. Хмельницький) та в освітній процес Хмельницького національного університету на кафедрі комп'ютерної інженерії та інформаційних систем і другої кафедри Другого навчально-наукового інституту Воєнної академії імені Євгенія Березняка.

6. Мова та стиль викладення результатів.

Дисертаційна робота написана українською мовою. Дисертація написана логічно та доступно на високому науковому рівні з використанням сучасної термінології. Матеріали дисертаційної роботи викладено послідовно, доступно для розуміння і сприйняття. Стиль мовлення задовольняє вимоги. Здобувач використав загальноприйняту термінологію.

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

Дисертаційна робота оформлена відповідно до вимог наказу МОН України від 12 січня 2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

7. Оприлюднення основних наукових результатів дисертаційної роботи.

Основні наукові результати дисертації опубліковані в 11 наукових працях, серед яких 6 статей, з яких 5 статей у фахових наукових журналах України, включених на дату опублікування до переліку наукових фахових видань України категорії Б, та однієї статті в міжнародному науковому журналі, що індексується в наукометричній базі Scopus (Q2), 5 праць в матеріалах міжнародних конференцій та семінарів, які проіндексовано у наукометричній базі Scopus. Також, опубліковано одне свідоцтво про

реєстрацію авторського права на твір (програму), в якому подано програмно-технічну реалізацію обманної системи.

У підсумку, опубліковані праці віддзеркалюють повноту викладу результатів дисертаційної роботи. Науковий рівень публікацій – високий. У всіх публікація здобувачем дотримано принципів академічної доброчесності.

Таким чином, наукові результати, подані в дисертаційній роботі, повністю висвітлені у наукових публікаціях здобувача.

8. Недоліки та зауваження до дисертаційної роботи:

1. В дисертації розглянуто лише один сценарій комп'ютерних атак, суть якого в цілеспрямованих комп'ютерних атаках з метою повної кластеризації об'єктів на два класи (реальні та хибні). Але не обгрунтовано поширення запропонованих підходів до інших сценаріїв КА.

2. Розділ 1 має нечітку тематичну організацію в параграфах. У ньому послідовно перелічуються десятки досліджень без належного групування за релевантністю (наприклад, варіанти MFO, оптимізація системи обману), що ускладнює виявлення прогалин в дослідженнях.

3. Метод виявлення комп'ютерних атак з використанням приманок і пасток згідно аналізу статистичних показників мережного трафіку стосується лише одного типу атак. Типів КА є багато і тоді при наповнення систем різними методами протидії різним типам КА може перевантажити їх та ускладнити функціонування, зокрема і в часі, що призведе до втрати актуальності результатів функціонування.

4. При обгрунтуванні показників для методу виявлення КА не наведено міжнародних стандартів і не показано повноту обраних показників.

5. З дисертації незрозуміло щодо відображення експериментів: реалістична динаміка атаки чи спрощені штучні сценарії.

6. У дисертації не проведено порівняльного аналізу запропонованого методу виявлення КА з існуючими рішеннями класу IDS/IPS на однакових наборах даних, що не дозволяє об'єктивно оцінити відносну ефективність розробленого підходу.

7. Результати першого експерименту, які відображені 17-ма слідами потенційних спіралей (рис. 4.4, с. 158, 159) відображають одну серію повторень і для подання потребують більшої кількості спроб дослідження щодо сталості дій.

Однак зазначені зауваження не є принциповими, істотно не впливають на зміст дисертаційної роботи та не знижують її наукової та практичної цінності.

9. Висновок про дисертаційну роботу.

Вважаю, що дисертаційна робота здобувача наукового ступеня доктора філософії Дрозда Андрія Ігоровича на тему «Методи та системи виявлення комп'ютерних атак в корпоративних мережах на основі популяційних алгоритмів» виконана на високому науковому рівні, не порушує принципів академічної доброчесності та є закінченим науковим дослідженням, сукупність теоретичних та практичних результатів якого розв'язує наукове завдання. Дисертаційна робота за актуальністю, практичною цінністю та науковою новизною повністю відповідає вимогам чинного законодавства України, що передбачені в п. 6-9 «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).

Офіційний опонент,
кандидат технічних наук, доцент
декан факультету комп'ютерних
інформаційних технологій
Західноукраїнського національного
університету Ігор ЯКИМЕНКО

Підпис Якименка
Завіряю:
НАЧАЛЬНИК
ЗАГАЛЬНОГО ВІДДІЛУ