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

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

Комп'ютерні атаки на корпоративні мережі постійно еволюціонують, а зловмисники добре обізнані з принципами роботи сучасних засобів захисту, оскільки ці рішення є комерційно доступними та піддаються аналізу. З часом їх ефективність знижується через передбачуваність поведінки. Тому актуальним є створення систем безпеки з недетермінованою логікою функціонування, що ускладнює їх дослідження та обходження.

Важливу роль у цьому відіграють обманні системи, приманки та пастки, які імітують реальні ресурси та відволікають зловмисників. Проте, через їх доступність, виникає потреба у постійному вдосконаленні їх архітектури та принципів роботи. Перспективним підходом є інтеграція таких засобів у єдині комплекси з централізованим керуванням і динамічною поведінкою.

Одним із шляхів досягнення недетермінованості є використання популяційних алгоритмів у підсистемах прийняття рішень. Вони дозволяють адаптивно обирати подальші дії системи залежно від ситуації в мережі, забезпечуючи як ефективність, так і складність прогнозування для зловмисника. Особливо перспективними є алгоритми, натхненні природними процесами, зокрема алгоритм молі і полум'я, який здатен уникати локальних оптимумів і здійснювати пошук глобально кращих рішень.

Однак більшість таких алгоритмів орієнтовані на неперервні області, тоді як вибір дій у системах захисту має дискретний характер. Це потребує адаптації алгоритмів до дискретного простору, розроблення відповідних моделей та функцій оцінювання.

Таким чином, актуальною науковою задачею є підвищення ефективності протидії комп'ютерним атакам шляхом створення обманних систем із недетермінованою поведінкою та оптимізацією їх дій на основі популяційних алгоритмів.

Дисертаційне дослідження виконувалось у рамках науково-дослідної тематики Хмельницького національного університету: 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); 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 автор дисертації був виконавцем.

2. Формулювання наукової задачі, мети й задачі дослідження

Здобувачем визначено та обгрунтовано протиріччя щодо удосконалення наявної архітектури чи розроблення принципово нової архітектури обманних систем, а також об'єкт і предмет дослідження.

Об'єктом дослідження є процес побудови та організації функціонування обманних систем із використанням приманок і пасток, призначених для своєчасного виявлення комп'ютерних атак і зловмисного програмного забезпечення в корпоративних мережах, з урахуванням їх динамічного та змінного характеру.

Предметом дослідження виступають методи та підходи до організації обманних систем із приманками і пастками, орієнтовані на підвищення ефективності виявлення комп'ютерних атак і зловмисного програмного забезпечення, а також на забезпечення адаптивності та стійкості таких систем у корпоративних мережах.

Метою дисертаційного дослідження є підвищення ефективності протидії комп'ютерним атакам і зловмисному програмному забезпеченню в корпоративних мережах шляхом оптимізації послідовності дій обманних систем із приманками і пастками на основі синтезу популяційних алгоритмів у центрах прийняття рішень, що забезпечує їх адаптивну та недетерміновану поведінку.

Для досягнення поставленої мети здобувачем було сформульовано такі основні завдання дослідження:

1) здійснити комплексний аналіз типів комп'ютерних атак і відповідного зловмисного програмного забезпечення, а також сучасних методів і систем їх виявлення в корпоративних мережах, включаючи обманні системи, приманки та пастки, і дослідити популяційні алгоритми, натхненні природними процесами, як основу для підвищення ефективності вибору та коригування дій таких систем;

2) розробити моделі комп'ютерних атак у корпоративних мережах з урахуванням наявності реальних і хибних об'єктів впливу, а також поведінки зловмисників, спрямованої на їх ідентифікацію та класифікацію;

3) сформувати формалізований опис архітектури обманних систем із приманками і пастками, що включає підсистему прийняття рішень на основі популяційних алгоритмів, зокрема алгоритму молі й полум'я, для оптимізації формування послідовності дій і їх динамічного коригування в умовах атак;

4) розробити метод синтезу дискретної модифікації алгоритму молі й полум'я в архітектурі обманних систем для забезпечення їх тривалого, адаптивного та ефективного функціонування під час протидії зловмисникам шляхом варіювання кроків обробки подій;

5) розробити метод організації функціонування обманних систем у корпоративних мережах на основі інтеграції популяційних алгоритмів, який забезпечує вибір оптимальних наступних дій системи та запобігає реалізації складних, зокрема двоцільових, атак;

6) розробити метод виявлення атак типу «відмова в обслуговуванні» на основі статистичних показників із урахуванням його інтеграції в компоненти обманних систем для підвищення точності та достовірності діагностики таких атак;

7) створити обманну систему з приманками і пастками, орієнтовану на виявлення двоцільових комп'ютерних атак, зокрема атак типу «відмова в обслуговуванні», та провести її експериментальне дослідження з метою оцінювання ефективності, покращення характеристик і подальшого практичного впровадження.

3. 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 комп'ютерних атак та дій зловмисного програмного забезпечення, 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

У вступі обґрунтовано актуальність задачі підвищення ефективності протидії зловмисним діям у корпоративних мережах шляхом удосконалення архітектури та методів функціонування обманних систем з приманками і пастками. Визначено доцільність використання обманних систем із застосуванням популяційних алгоритмів, наведено зв'язок із науковими дослідженнями, а також подано основні результати роботи та їх практичне впровадження.

У першому розділі проаналізовано предметну область, існуючі обманні системи, приманки й пастки, а також методи виявлення комп'ютерних атак і зловмисного програмного забезпечення. Розглянуто популяційні алгоритми та їх характеристики.

У другому розділі розроблено моделі двоцільових атак і запропоновано удосконалену архітектуру обманних систем з приманками і пастками із використанням популяційних алгоритмів, зокрема алгоритму молі й полум'я, що дозволяє оптимізувати вибір наступних дій, уникати повного перебору, враховувати зміни середовища та протидіяти складним атакам.

У третьому розділі запропоновано метод синтезу в архітектурі обманних систем з приманками і пастками алгоритму дискретної оптимізації молі й полум'я з формуванням дискретного простору пошуку, що забезпечує адаптивність і запобігає збіжності до локальних оптимумів. Також розроблено метод організації функціонування обманних систем, який забезпечує автономний вибір дій, ускладнює дії зловмисників і дозволяє динамічно керувати компонентами мережі.

У четвертому розділі представлено метод виявлення атак типу «відмова в обслуговуванні» на основі статистичного аналізу мережного трафіку, що підвищує точність і швидкість їх виявлення. Описано програмну реалізацію системи, проведені експерименти та оцінено її ефективність.

У висновках узагальнено наукові та практичні результати дослідження. У додатках наведено публікації, акти впровадження та фрагменти програмного забезпечення.

5. Обґрунтованість і достовірність наукових положень, висновків і рекомендацій

Наукові положення, висновки та рекомендації, які сформульовані в дисертаційній роботі, є обґрунтованими завдяки коректному й доцільному застосуванню математичного апарату, зокрема розробленої архітектури обманних систем з приманками і пастками та їх окремих компонентів, а також моделей комп'ютерних атак, спрямованих як на реальні, так і на хибні об'єкти корпоративних мереж. Запропоновані моделі враховують специфіку поведінки зловмисників і особливості функціонування обманних компонентів у змінному мережному середовищі.

Достовірність результатів підтверджується також практичною реалізацією розробленої обманної системи, яка включає серверну та клієнтську частини програмного забезпечення. Ці компоненти забезпечують повноцінну організацію функціонування системи, керування приманками і пастками, а також обробку як штатних, так і позаштатних подій у корпоративних мережах. У межах реалізації в архітектуру системи інтегровано метод виявлення комп'ютерних атак, що базується на аналізі статистичних показників мережного трафіку, що підвищує точність і оперативність реагування.

Важливим підтвердженням обґрунтованості отриманих результатів є їх практичне впровадження на підприємствах, які використовують сучасні засоби захисту корпоративних мереж. Отримані результати демонструють узгодженість теоретичних положень із практичними наслідками їх застосування, що свідчить про ефективність запропонованих рішень та їх придатність до використання в реальних умовах.

6. Практичне значення одержаних результатів

Розроблено обманну систему з приманками і пастками, призначену для виявлення комп'ютерних атак і зловмисного програмного забезпечення в корпоративних мережах. Ключовою особливістю цієї системи є використання підсистеми прийняття рішень, у якій вибір подальших дій та їх динамічне коригування здійснюється на основі алгоритму дискретної оптимізації молі і полум'я. Додатково в її архітектуру інтегровано метод виявлення комп'ютерних атак, що базується на аналізі статистичних показників мережних процесів, що дозволяє підвищити точність і своєчасність виявлення загроз.

Синтез популяційних алгоритмів у структурі обманних систем для підтримки процесу прийняття рішень забезпечив можливість формування таких послідовностей дій системи, які є складними для прогнозування та аналізу з боку зловмисників. Це сприяє підвищенню рівня їх дезорієнтації під час здійснення атак. У процесі інтеграції алгоритму молі і полум'я було не лише адаптовано його до умов дискретного простору пошуку, але й деталізовано основні етапи його функціонування з урахуванням специфіки задач вибору дій у корпоративних мережах. Отримані результати створюють основу для подальшого застосування та адаптації інших популяційних алгоритмів, натхненних природними процесами, до аналогічних задач.

Результати експериментальних досліджень підтвердили, що запропонована обманна система забезпечує стабільне та коректне функціонування в умовах динамічних змін середовища корпоративних мереж. Система демонструє ефективне використання приманок і пасток для виявлення інфікованих програмних компонентів, а також здатність адаптивно формувати та обирати наступні кроки функціонування залежно від поточного стану мережі та характеру виявлених загроз.

7. Особистий внесок здобувача

Особистий внесок здобувача полягає у самостійному отриманні та розвитку теоретичних і практичних результатів, спрямованих на підвищення ефективності

функціонування обманних систем у корпоративних мережах при виявлення двоцільових КА. Здобувачем розроблено метод виявлення комп'ютерних атак типу «відмова в обслуговуванні», який базується на аналізі статистичних показників мережного трафіку, а також запропоновано метод організації функціонування обманних систем із приманками і пастками в корпоративних мережах. Також, здобувачу належать ключові наукові ідеї, постановка задач, обґрунтування підходів та основні результати теоретичних і практичних досліджень. Зокрема, автором розроблено архітектуру обманних систем із використанням популяційних алгоритмів у підсистемі прийняття рішень для вибору наступних кроків функціонування, запропоновано метод синтезу популяційних алгоритмів в архітектурі обманних систем з приманками і пастками, включаючи алгоритм дискретної оптимізації молі і полум'я; визначено підходи до оцінювання рівня кібербезпеки вузлів корпоративних мереж; обґрунтовано стратегії застосування штучних нейронних мереж для виявлення бот-мереж, а також тестування безпеки застосунків. Крім того, автором проведено аналіз засобів для реалізації бінарної класифікації, визначено статистичні показники комп'ютерних атак на основі мережного трафіку та досліджено параметри операційних систем реального часу, що впливають на стан операційного середовища. Також здобувачем розроблено архітектуру програмного забезпечення обманних систем і реалізовано відповідний програмний код із використанням популяційних алгоритмів для підтримки процесів прийняття рішень.

8. Апробація матеріалів дисертації

Апробацію основних положень, ідей, висновків дисертаційної роботи проведено на науковому семінарі кафедри комп'ютерної інженерії та інформаційних систем у Хмельницькому національному університеті. Наукові результати роботи доповідалися на міжнародних та всеукраїнських науково-практичних конференціях: 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).

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

10. Зауваження

У результаті розгляду дисертації сформовано наступні зауваження та рекомендації.

1. Виклад матеріалу першого розділу дисертації переважно здійснюється на основі повторюваної структури «В [х], [опис]» для представлення аналізу літератури. Таке жорстке форматування зменшує читабельність і не дозволяє відрізнити фундаментальні роботи від другорядних досліджень.

2. В дисертації недостатньо чітко окреслено відмінність власного варіанту алгоритму дискретної оптимізації молі і полум'я від відомих варіантів, які використано раніше.

3. Обмеження, які пов'язані з ресурсами, додатковими витратами на систему та швидкістю реагування в режимі реального часу, згадуються концептуально, але формально не включені в модель оптимізації.

4. Зіставлення між змінними оптимізації та конкретними системними діями, такими як конкретні конфігурації приманки або пастки недостатньо чітко пояснено.

5. Вибір набору даних CIC-IDS2017 для оцінки методу виявлення КА не обґрунтовано з точки зору його репрезентативності щодо сучасних векторів атак, оскільки зазначений датасет містить трафік, згенерований у 2017 році і може не відображати актуальні характеристики атак типу DoS.

6. Набір даних, середовище моделювання або мережні сценарії, що використовуються для оцінки, описані недостатньо деталізовано в дисертації.

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

11. Загальний висновок

Вважаю, що дисертаційна робота Дрозда Андрія Ігоровича на тему «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 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 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 технічних наук, доцент,
завідувач кафедри кібербезпеки
Хмельницького національного університету _____ Юрій КЛЬОЦ

«Підпис Юрія КЛЬОЦА засвідчую»:
Проректор з наукової роботи
Хмельницького національного університету _____ Олег СИНЮК