

САВЕНКО Олег

Хмельницький національний університет

<https://orcid.org/0000-0002-4104-745X>

e-mail: savenko_oleg_st@ukr.net

ДРОЗД Андрій

Хмельницький національний університет

<https://orcid.org/0009-0008-1049-1911>

e-mail: andriydrozdit@gmail.com

КОРОБЧИНСЬКИЙ Максим

Воєнно-дипломатична академія імені Євгенія Березняка

<https://orcid.org/0000-0001-8049-4730>

e-mail: maks_kor@ukr.net

МЕТОД СИНТЕЗУ ПОПУЛЯЦІЙНИХ АЛГОРИТМІВ В АРХІТЕКТУРІ ОБМАННИХ СИСТЕМ З ПРИМАНКАМИ І ПАСТКАМИ

У роботі розроблено новий метод синтезу алгоритму дискретної оптимізації молі й полум'я в архітектурі обманних систем з приманками і пастками. На відміну від відомих підходів, запропонований метод забезпечує формування дискретного простору пошуку з координатним поданням об'єктів, синтез спірального сліду на основі динамічного переміщення молі й полум'я для уникнення передчасної збіжності до локальних оптимумів.

Постановка задачі вибору наступних кроків обманних систем, що включає керування приманками і пастками та їх коригування в процесі реагування на події, розглядається як оптимізаційна задача. Її метою визначено підвищення ефективності виявлення комп'ютерних атак і зловмисного програмного забезпечення в корпоративних мережах. Змінюваними параметрами виступають кроки роботи обманних систем, моделі процесів та архітектурні особливості, а обмеженнями — характеристики операційного середовища корпоративних мереж.

Запропонований метод дає змогу забезпечити знаходження оптимальної послідовності кроків у змінюваних умовах, включно з можливістю їх оперативної адаптації до дій зловмисника. Це, у свою чергу, уможливорює створення обманних систем, здатних до тривалого автономного функціонування без постійного залучення адміністраторів та з підвищеною стійкістю до розпізнавання їх принципів роботи зловмисниками.

Проведені експерименти показали перспективність запропонованого напрямку досліджень та синтезу в архітектурі обманних систем популяційних алгоритмів для оптимізації вибору ними подальших кроків.

Перспективи подальших досліджень полягають у поглибленні інтеграції популяційних алгоритмів в архітектуру обманних систем з приманками та пастками, а також у розробленні методу організації їхнього функціонування відповідно до запропонованої концептуальної моделі. Результати роботи спрямовані на підвищення рівня кіберзахисту корпоративних мереж через створення інтелектуальних адаптивних систем протидії сучасним КА та діям ЗПЗ.

Ключові слова: корпоративні мережі; комп'ютерні станції; системи обману; популяційні алгоритми; алгоритм молі й полум'я; дискретна оптимізація; пастка; приманка; зловмисне програмне забезпечення; комп'ютерні атаки; архітектура систем.

SAVENKO Oleg, DROZD Andriy

Khmelnytskyi National University

KOROBCHYNSKYI Maksym

Yevhenii Bereznyak Military Academy

METHOD OF SYNTHESIS OF POPULATION ALGORITHMS IN THE ARCHITECTURE OF DECEPTIVE SYSTEMS WITH BAITS AND TRAPS

In the work, a new method of synthesis of the algorithm of discrete optimization of moth and flame in the architecture of deceptive systems with decoys and traps is developed. In contrast to known approaches, the proposed method provides the formation of a discrete search space with a coordinate representation of objects, the synthesis of a spiral trace based on the dynamic movement of the moth and flame to avoid premature convergence to local optima.

Setting the problem of choosing the next steps of deception systems, which includes the management of decoys and traps and their adjustment in the process of responding to events, is considered as an optimization problem. Its purpose is to increase the effectiveness of detection of computer attacks and malicious software in corporate networks. The changing parameters are the operating steps of deception systems, process models, and architectural features, and the limitations are the characteristics of the operating environment of corporate networks.

The proposed method makes it possible to ensure finding the optimal sequence of steps in changing conditions, including the possibility of their operational adaptation to the attacker's actions. This, in turn, enables the creation of deceptive systems capable of long-term autonomous functioning without the constant involvement of administrators and with increased resistance to recognition of their working principles by attackers.

The conducted experiments showed the prospects of the proposed direction of research and synthesis in the architecture of deceptive systems of population algorithms for optimizing their choice of further steps.

Prospects for further research are in deepening the integration of population algorithms into the architecture of deceptive systems with baits and traps, as well as in developing a method of organizing their functioning in accordance with the proposed

conceptual model. The results of the work are aimed at increasing the level of cyber protection of corporate networks through the creation of intelligent adaptive systems for countering modern self-propelled missiles and anti-aircraft weapons.

Keywords: corporate networks; computer stations; fraud systems; population algorithms; moth and flame algorithm; discrete optimization; trap; lure; malicious software; computer attacks; systems architecture.

Стаття надійшла до редакції / Received 16.04.2025

Прийнята до друку / Accepted 11.05.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Перспективним напрямом для забезпечення безпеки та захисту корпоративних мереж є використання обманних систем, приманок і пасток [1, 2]. Такі рішення є дорого вартісними і прийняття рішень щодо них пов'язане з особливостями в потребах забезпечення надійнішої безпеки та захисту в корпоративних мережах [3, 4]. Зловмисники можуть з часом адаптуватись до таких систем і, тому, для їх тривалої експлуатації необхідно, щоб вони мали спроможність функціонувати тривалий час, тобто по падати в стан збіжності, та приймати рішення самостійно без залучення адміністраторів [5, 6].

Вибір наступних кроків [1, 3] в обманних системах, які також включають керування приманками і пастками, та їх зміни чи коригування протягом виконання певних послідовностей кроків відповідає постановці задачі оптимізації, суть якої полягає у виборі найкращого (оптимального) варіанта з великої кількості можливих. Оптимальним значенням буде найкращий із можливих варіантів, який максимально відповідає певним умовам, вимогам чи завданню, забезпечуючи найвигідніший, найефективніший чи найбільш підходящий результат.

Задачу оптимізації з вибору наступних кроків обманних систем з приманками і пастками в корпоративних мережах сформулюємо згідно досягнення підвищення ефективності виявлення КА і ЗПЗ як критерію оптимальності, змінюваності кроків обманних систем як змінюваних параметрів систем, моделей процесів та архітектури обманних систем в корпоративних мережах, а також обмежень щодо операційного середовища корпоративних мереж і особливостей обманних систем з приманками і пастками. Для її розв'язування потрібен вибір методу, яким би можна було забезпечити знаходження оптимального значення, тобто послідовності кроків систем в змінюваному середовищі корпоративних мереж під час КА чи дій ЗПЗ та із можливістю їх поточної зміни, пов'язаної із потребою коригування відповіді систем на впливи.

Тому, актуальною науковою задачею є синтез в обманних системах таких методів оптимізації, які б забезпечили їх тривале функціонування без залучення адміністраторів та реакції на події, які викликані впливами комп'ютерних атак (КА) чи дій зловмисного програмного забезпечення (ЗПЗ), таким чином, щоб принципи функціонування систем були складно зрозумілими для зловмисників.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Вибір наступних кроків в обманних системах, які також включають керування приманками і пастками, та їх зміни чи коригування протягом виконання певних послідовностей кроків відповідає постановці задачі оптимізації, суть якої полягає у виборі найкращого (оптимального) варіанта з великої кількості можливих. Оптимальним значенням буде найкращий із можливих варіантів, який максимально відповідає певним умовам, вимогам чи завданню, забезпечуючи найвигідніший, найефективніший чи найбільш підходящий результат.

Задачу оптимізації з вибору наступних кроків обманних систем з приманками і пастками в корпоративних мережах сформулюємо згідно досягнення підвищення ефективності виявлення КА і ЗПЗ як критерію оптимальності, змінюваності кроків обманних систем як змінюваних параметрів систем, моделей процесів та архітектури обманних систем в корпоративних мережах, а також обмежень щодо операційного середовища корпоративних мереж і особливостей обманних систем з приманками і пастками. Для її розв'язування потрібен вибір методу, яким би можна було забезпечити знаходження оптимального значення, тобто послідовності кроків систем в змінюваному середовищі корпоративних мереж під час КА чи дій ЗПЗ та із можливістю їх поточної зміни, пов'язаної із потребою коригування відповіді систем на впливи.

Оптимізація відноситься до процесу пошуку найкращого можливого рішення чи рішень для певної проблеми [7]. У міру зростання складності проблем, за останні кілька десятиліть, потреба в нових методах оптимізації стає більш очевидною, ніж раніше. До появи евристичних методів оптимізації застосовували математичні методи оптимізації, які в основному детерміновані і, тому, страждають проблемою, суть якої в збіжності пошуку в локальних оптимумах. З появою методів, які базуються на використанні популяційних алгоритмів, задачі оптимізації можна розв'язувати з досягненням оптимального або субоптимального розв'язків.

Популяційні алгоритми є класом метаевристичних методів оптимізації, які спрямовані на сукупність (популяцію) розв'язків. Вони імітують природні процеси. Популяційні алгоритми переважно класифікують [7] на три основні категорії в залежності від джерел натхнення: еволюція; фізика; рій. Еволюційні алгоритми

імітують еволюційні процеси в природі (наприклад, генетичні алгоритми, алгоритм еволюційної мембрани). Кількість алгоритмів на основі рою (наприклад, алгоритм бджіл, оптимізатор сірого вовка) більша, ніж еволюційних. Третій клас алгоритмів натхненний фізичними явищами в природі (наприклад, алгоритм гравітаційного пошуку, оптимізація хімічних реакцій). Відомі, також, популяційні алгоритми [7] з різними джерелами натхнення: неживою природою; живою природою. Обмежитись декількома популяційними алгоритмами при розв'язуванні задач оптимізації складно, оскільки не існує одного чи декількох популяційних алгоритмів оптимізації для розв'язування всіх оптимізаційних завдань [7].

Розглянемо поширені популяційні алгоритми, які використовують для розв'язування оптимізаційних задач.

В роботі [8] запропоновано підхід до постановки та розв'язування задачі оптимального вибору показників якості продукції в системі «виробник–споживач» на основі нечітких когнітивних карт і генетичного алгоритму з урахуванням інтересів як виробника, так і споживача. Критерієм оптимізації є максимальна наближеність між привабливістю товару та бажанням його придбати. Контрольованими змінними є рівні показників виробника та споживача. Обмеженнями є домовленості щодо необхідних рівнів показників, які спільні для виробника і споживача. Нечіткі когнітивні карти використовуються для побудови залежності, зокрема з відображенням в цільовій функції, а оптимальні рішення знаходяться за допомогою генетичного алгоритму.

В роботі [9] запропоновано генетичний алгоритм пошуку набору правил для формування нечіткої бази знань, яка збалансована за критеріями точності та компактності. Відмінністю цього генетичного алгоритму від відомих реалізацій є введення в постановку задачі оптимізації лінійного обмеження, яке задає рівень компенсації точності моделі її компактністю, що дає змогу наближувати область допустимих розв'язків до парето-фронту.

В роботі [10] здійснено впровадження процедури кластеризації масивів даних на основі вдосконаленого алгоритму сірого вовка. Перевагою запропонованого підходу є скорочення часу вирішення задач оптимізації в умовах перекриття кластерів. Особливістю запропонованого методу є велика швидкість, завдяки тому, що увесь масив обробляється лише один раз, тобто усувається необхідність багаторазового самонавчання, реалізованого в традиційних алгоритмах нечіткої кластеризації. В роботі [11] запропоновано метод кластеризації масивів даних на основі комбінованої оптимізації функцій щільності розподілу та еволюційного методу котячих роїв. Перевагою запропонованого підходу є скорочення часу вирішення оптимізаційних задач в умовах перекриття кластерів. В роботі [12] розглянуто проблему нечіткої кластеризації великих масивів даних, які надсилаються на обробку як у пакетному, так і в онлайн режимах, на основі достовірного підходу. Щоб знайти глобальний екстремум цільової функції достовірної нечіткої кластеризації, була введена модифікація роєвого алгоритму зграй божевільних кішок, яка поєднує в собі переваги еволюційних алгоритмів і глобального випадкового пошуку. Показано, що різні режими пошуку генеруються єдиною математичною процедурою, деякі випадки якої є відовими алгоритмами як локальної, так і глобальної оптимізації. Запропонований характеризується великою швидкістю та надійністю в задачах багатоекстремальної нечіткої кластеризації. Таким чином, для однієї типової задачі щодо кластеризації в масивах даних застосовано різні популяційні алгортми, які дали змону ефективно розв'язати задачі оптимізації.

В роботі [13] подано різні прикладні методи комбінаторної оптимізації, а також розглянуто питання формалізації, класифікації та розв'язування задач метаевристичними методами.

В роботі [14] запропоновано новий природний алгоритм, в якому імітується механізм полювання мурашиних левів у природі. Реалізовано п'ять основних кроків полювання на здобич, таких як випадкова хода мурах, створення пасток, захоплення мурах у пастки, ловля здобичі та повторне будівництво пасток.

В роботі [15] запропонована нова метаевристика натхненна сірими вовками. Алгоритм імітує ієрархію лідерства та механізм полювання сірих вовків у природі. Чотири типи сірих вовків, такі як альфа, бета, дельта та омега, використовуються для імітації ієрархії лідерства. Крім того, реалізовано три основні етапи полювання, пошуку здобичі, оточення здобичі та нападу на здобич. Потім алгоритм перевіряється на основі 29 відомих тестових функцій, а результати перевіряються шляхом порівняльного дослідження за допомогою оптимізації роєм частинок, алгоритму гравітаційного пошуку, диференціальної еволюції, еволюційного програмування і стратегії еволюції. Алгоритм здатний забезпечити конкурентоспроможні результати порівняно з відовими метаевристичними методами.

В роботі [7] запропоновано нову парадигму оптимізації, яка натхненна живою природою, і називається алгоритмом оптимізації молі і полум'я. Основним джерелом натхнення для цього оптимізатора є метод навігації метеликів молі у природі, який називається поперечною орієнтацією. Метелики літають вночі, зберігаючи фіксований кут відносно місяця, що є дуже ефективним механізмом для подорожей по прямій лінії на великі відстані. Однак ці комахи потрапляють в пастку на смертоносну спіраль навколо штучного світла. В роботі математично змодельовано цю поведінку для виконання оптимізації. Алгоритм порівнюється з іншими відовими природними алгоритмами на 29 тестових і 7 реальних інженерних задачах. Статистичні результати порівняльних функцій показують, що цей алгоритм здатний забезпечити конкурентоспроможні результати.

Крім того, результати реальних задач демонструють переваги цього алгоритму у вирішенні складних задач із обмеженими та невідомими просторами пошуку. В роботі [15] розглянуто проблеми автоматизації побудови класифікаційних дерев на основі схеми відбору розгалужених ознак. Об'єктом дослідження є класифікаційні дерева. Предметом дослідження є методи, алгоритми та схеми побудови класифікаційних дерев. Метою роботи є побудова ефективного методу для синтезу моделей дерева класифікації на основі групової оцінки важливості дискретних ознак у межах розгалуженого вибору ознак. Запропоновано метод побудови дерев класифікації, який для заданої навчальної вибірки визначає індивідуальну інформативність груп ознак та їх комбінацій по відношенню до початкового значення функції класифікації. Розроблений метод логічного дерева при побудові наступного вузла дерева класифікації намагається виділити групу найбільш тісно пов'язаних між собою дискретних ознак, що зменшує загальну структурну складність моделі, прискорює обчислення при розпізнаванні об'єктів на основі моделі, а також підвищує узагальнюючі властивості моделі. Таким чином, запропонований підхід в роботах [7, 16] дає змогу коригувати наступні групи показників. В роботі [17] об'єктом дослідження є методика оцінки показника інформаційної безпеки. Розглянуто проблему уніфікації та спрощення процесів оцінки ступеня інформаційної безпеки з метою зменшення залучення в них людських і матеріальних ресурсів, використовуючи апарат теорії нечітких множин для врахування висновків компетентних експертів. Розроблено нечітку продукційну модель оцінки ступеня інформаційної безпеки, яка базується на використанні експертних знань та методів нечіткої логіки. Запропоновано поетапний підхід до визначення потенційних ризиків, їх класифікації за категоріями та розрахунку коефіцієнтів впливу. Створено ітераційний метод оцінки, який дозволяє отримати числовий показник ступеня інформаційної безпеки. Розроблено евристичні правила визначення ефективної оцінки ступеня інформаційної безпеки з урахуванням коефіцієнта критичності та коефіцієнтів впливу різних категорій ризику.

В роботі [18] описано приклад оптимізації лінії виробництва двигуна на основі моделювання в реальному світі. Оптимізація спрямована на максимізацію використання машин і водночас мінімізацію зв'язаного капіталу шляхом маніпулювання 56 унікальними змінними рішень. Для цього використано метаввристичний алгоритм молі і полум'я, який отримав успішні результати в різних проблемних областях.

В роботі [19] представлено алгоритм оптимізації молі і полум'я. Він застосовується для вирішення складних реальних проблем оптимізації в багатьох областях. У роботі подано широкий огляд варіантів цього алгоритму, включаючи класичну версію, двійкові типи, модифіковані версії, гібридні версії, багатоцільові версії та прикладну частину алгоритму у різних секторах.

В роботі [20] алгоритм молі і полум'я демонструє кращі результати продуктивності порівняно з іншими розглядуваними метаввристичними алгоритмами для вирішення проблем глобальної оптимізації з нелінійними обмеженнями. Однак він все ще страждає від отримання якісного рішення та низької швидкості конвергенції.

В роботі [21] технологічний процес вважається багатоаспектним, якщо має місце ряд дефектів різного типу, які виявляються та усуваються одночасно в процесі виконання процесу. Якість технологічного процесу оцінюється ймовірністю вихідних нульових дефектів, а також ймовірностями нульових дефектів для кожного з типів дефектів. Завдання оптимізації передбачають вибір такої структури процесу, яка забезпечить необхідний вихідний рівень якості продукції за певних витратних обмежень. Задача оптимізації розв'язується за допомогою генетичних алгоритмів, які дозволяють знаходити наближене до глобального оптимальне рішення.

В роботі [22] розглядається теорія та застосування мурашиних алгоритмів, нові методи дискретної оптимізації на основі моделювання самоорганізованої колонії біологічних мурах. Колонію розглянуто як багатоагентну систему, де кожен агент функціонує незалежно за простими правилами. На відміну від майже примітивної поведінки агентів, поведінка всієї системи виявляється розумною. Мурашині алгоритми були успішно застосовані для розв'язування багатьох складних задач комбінаторної оптимізації, таких як задача комівояжера, задача маршрутизації транспортного засобу, задача розфарбовування графа, задача квадратичного призначення, задача оптимізації мережного трафіку, задача планування роботи в магазині тощо. Мурашині алгоритми особливо ефективні для онлайн-оптимізації процесів у розподілених нестационарних системах (наприклад, телекомунікаційна мережа). маршрутизація).

В роботі [23] розглянуто гібридний фільтр активної потужності. Щоб отримати його більш точні параметри, запропоновано новий популяційний метод на основі алгоритму молі і полум'я. Його модифікація в тому, що здійснено поділ на групу експлуатації та групу дослідження.

В роботі [24] отримання відповідних параметрів фотоелектричних моделей на основі вимірних даних про струм та напругу фотоелектричної системи є важливим для оцінки, керування та оптимізації фотоелектричних систем. Щоб отримати конкретні параметри фотоелектричних моделей, запропоновано метаввристичний алгоритм оптимізації молі і полум'я та симбіотичної еволюції. Запропонований підхід поділяє популяцію на дві паралельні робочі підгрупи.

В роботі [25] традиційна робота водосховища з виробництва електроенергії в основному передбачає максимізацію виробництва електроенергії та гарантує стабільність енергосистеми. Однак, розглядаючи цілі виробництва електроенергії, можна ігнорувати її вплив на екологічне середовище та навігацію. Створено

багатоцільову модель оптимізації, яка враховує цілі виробництва електроенергії, екології та навігації. Для ефективного розв'язання моделі було запропоновано новий покращений багатоцільовий алгоритм оптимізації молі і полум'я на основі домінування. Щоб підвищити здатність алгоритму оптимізації молі і полум'я подолати потрапляння в локальний оптимум, його було вдосконалено в трьох аспектах: формула оновлення; натхнення лінійної траєкторії польоту молі; стратегія оновлення популяції полум'я. Щоб відрізнити цих індивідів, які не домінують один над одним у домінуванні Парето, було запропоновано домінування в поєднанні з контрольними точками.

В роботі [26] пропонується нова схема навчання для машини екстремального навчання ядра, як базується на використанні стратегії хаотичної оптимізації молі і полум'я. У запропонованій схемі одночасно здійснюється оптимізація параметрів і вибір ознак.

В роботі [27] запропоновано вдосконалений алгоритм оптимізації молі і полум'я, щоб полегшити проблеми передчасної збіжності до локальних мінімумів. З точки зору різноманітності, вага інерції контролю зворотного зв'язку різноманітності введена в оптимізацію полум'я молі, щоб збалансувати використання алгоритму та можливості глобального пошуку. Крім того, додається невелика мутація ймовірності після етапу оновлення позиції для покращення ефективності оптимізації.

В роботі [28] розглянуто алгоритм оптимізації молі і полум'я як новий метаевристичний алгоритм на основі сукупності для вирішення проблем глобальної оптимізації. Генерація полум'я та спіральний пошук є двома ключовими компонентами, які впливають на продуктивність алгоритму. Для покращення різноманітності полум'я та пошукової здатності молі запропоновано вдосконалений алгоритм оптимізації молі і полум'я. Основними особливостями його є такі: полум'я генерується ортогональним опозиційним навчанням; модифіковано механізм оновлення позиції молі з лінійним пошуком і оператором мутації.

В роботі [29] проаналізовано проблему відбору генів, яка пов'язана з великою кількістю генів (релевантних, надлишкових або шумових), що потребують ефективного методу, щоб допомогти у виявленні захворювань. У цій задачі обчислювальна складність зменшується шляхом вибору невеликої кількості генів, але необхідно вибрати відповідні гени, щоб зберегти високий рівень точності. Тому, щоб знайти оптимальну підмножину генів, представлено алгоритм ройового інтелекту для відбору генів, який називається квантовим алгоритмом оптимізації молі і полум'я, який базується на комбінуванні між квантовими обчисленнями та алгоритмом оптимізації молі і полум'я.

Таким чином, використання популяційних алгоритмів для розв'язування задач оптимізації є перспективним. Серед багатьох популяційних алгоритмів наявний клас таких алгоритмів натхнений живою природою, з якого можуть бути використані алгоритми для синтезу в архітектурі обманних систем з приманками і пастками, оскільки їх поведінку, тобто підібрані наступні кроки для виконання, буде складно зрозуміти зловмисникам.

Метою роботи є покращення функціонування обманних систем з приманками і пастками в корпоративних мережах за рахунок синтезу в їх архітектурі популяційних алгоритмів для заплутування зловмисників та підтримування тривалих відповідей систем на впливи, що викликані КА та діями ЗПЗ.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

В архітектурі обманних систем з приманками і пастками здійснення синтезу популяційних алгоритмів, зокрема алгоритму молі і полум'я, є необхідним для оптимізації послідовності наступних кроків при їх формуванні. Під час здійснення КА та дій ЗПЗ необхідно забезпечити в таких системах уникнення повного перебору варіантів, швидкої збіжності обраних кроків при триваючих впливах та зміну послідовності кроків з врахуванням поточних змін в оточуючому середовищі корпоративних мереж, а також врахування потенційних спроможностей зловмисників до здійснення двоцільових КА. Тому, здійснимо спочатку розроблення методу вибору кроків обманних систем з приманками і пастками на основі алгоритму молі і полум'я як частини забезпечення їх функціонування.

Вибір популяційних алгоритмів в архітектурі обманних систем відповідає завданням, які необхідно вирішувати в них, що пов'язані з невідомими та обмеженими просторами пошуку варіантів наступних кроків. Їх використовують для уникнення передчасної збіжності, щоб оптимізація забезпечила збіжність до глобального оптимуму. Для цього може бути використано набір рішень, які можуть бути сформовані завдяки наявності ресурсів обманних систем, зокрема певної кількості приманок і пасток, а також можливості формування багатьох варіантів наступних кроків систем.

Процес оптимізації при виборі рішень поділимо на два етапи: дослідження наявних варіантів; застосування обраних варіантів. На етапі дослідження з простору пошуку обираємо варіант послідовності кроків, формуючи вектор наступних кроків обманних систем. На етапі застосування обраних варіантів здійснюємо виконання обраних кроків та покращення обраного варіанту через послідовності наступних кроків з метою наближення до глобального оптимуму. Застосування такого поділу процесу оптимізації на два етапи є можливим, оскільки тривалість КА чи дій ЗПЗ та їх змінюваність потребують гнучкої реакції на зміну оточуючого середовища корпоративних мереж. Процес оптимізації з розділенням на два етапи зображено на рис. 1.

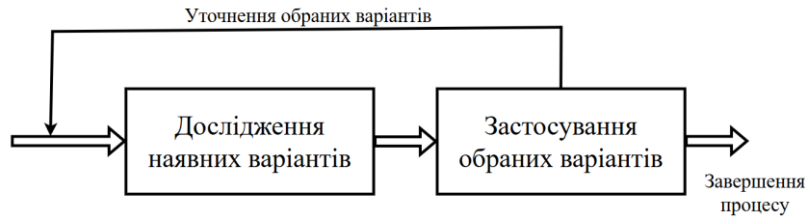


Рис. 1. Поділ процесу оптимізації на два етапи

Таким чином, спочатку в обманній системі буде сформовано вектор $v_{os,i}$ певною заданою послідовністю кроків для забезпечення реакції на впливи в корпоративних мережах від КА чи дій ЗПЗ і це буде відповідати етапу дослідження наявних варіантів. На етапі застосування обраних варіантів частина кроків буде виконана обманною системою і в процес виконання будуть закладені кроки для оцінювання поточного стану в корпоративних мережах, стану системи та результативності кроків. Згідно опрацьованої такої інформації буде здійснено уточнення обраних варіантів кроків і сформовано новий вектор наступних кроків системи так:

$$v_{os,i,u} = (v_{os,i,u,1}, v_{os,i,u,2}, \dots, v_{os,i,u,N_{os,i,u}}), \quad (1)$$

де $v_{os,i,u,j}$ – крок обманної системи з приманками і пастками; $j = 1, 2, \dots, N_{os,i,u}$; $N_{os,i,u}$ – кількість кроків обманних систем з приманками і пастками для вирішення певного завдання, які визначено системою в поточний момент часу; i – i -та послідовність кроків для вирішення певного завдання системи; u – уточнення кроків, які задано вектором $v_{os,i}$.

Введемо цільову функцію оцінювання обраних варіантів так:

$$F_{os}(v_{os,i}, v_{os,i,u}) \rightarrow [0; 1], \quad (2)$$

де $v_{os,i,u,j}$ – крок обманної системи з приманками і пастками; $j = 1, 2, \dots, N_{os,i,u}$; $N_{os,i,u}$ – кількість кроків обманних систем з приманками і пастками для вирішення певного завдання, які визначено системою в поточний момент часу; i – i -та послідовність кроків для вирішення певного завдання системи; u – уточнення кроків, які задано вектором $v_{os,i}$.

Кращим результатом оцінювання згідно цільової функції F_{os} (формула (2)) приймемо більше з її двох значень. Цільова функція F_{os} (формула (2)) дає оцінку уточненого варіанту послідовності кроків, який буде формувати вектор $v_{os,i,u}$ і відповідає в процесі оптимізації за уточнення обраних варіантів (рис. 1). На початку вибору рішення, коли здійснюється дослідження наявних варіантів, вона теж застосовується, але її аргументи будуть однакові, тоді вона оцінює обраний варіант, який фіксується в обманній системі. Частина кроків, які задано вектором $v_{os,i}$ може бути повторена у векторі $v_{os,i,u}$. Застосування цільової функції буде до того часу, поки триває КА чи дії ЗПЗ, що потребуватиме формування відповідних дій обманних систем з приманками і пастками. Послідовності кроків систем будуть змінюватись і кожного разу будуть оцінюватись цільовою функцією та прямувати до досягнення глобального оптимуму. Така схема відповідає загальній структурі популяційних алгоритмів.

Задамо функцію кодування об'єктів корпоративних мереж на координатній площині з врахуванням їх різних типів:

$$F_{os,kod}: (M_{kn,v,p,z,vect}, O_{kn}) \rightarrow M_{os,kod}(X_1, X_2, \dots, X_{N_{kn,v,p,z}}, K_{os}), \quad (3)$$

де $M_{os,kod}$ – матриця з координатами об'єктів корпоративних мереж та відомостями про тип об'єктів; K_{os} – код типу об'єктів корпоративних мереж; $K_{os} = \{k_{kod,1}, k_{kod,2}, \dots, k_{kod,N_{kn,v,p,z}}\}$; O_{kn} – тип об'єктів корпоративних мереж; X_j – вектор j – координат; $m_{kn,v,p,z,vect,i,j}$ – компонента вектору з елементів підмножини $M_{kn,v,p,i}$ ($i = 1, 2, \dots, N_{kn,v,p}$; $N_{kn,v,p}$ – кількість підмножин вузлів корпоративних мереж в множині $M_{kn,p}$); $N_{kn,v,p,z}$ – максимальна кількість вузлів в сегментах мережі включно з маршрутизатором; j – номер стовпця матриці; $j = 1, 2, \dots, N_{kn,v,p,z,N_{kn,v,p,z,j}}$; $j = 1, 2, \dots, N_{kn,v,p,z,j}$; $N_{kn,v,p,z,j}$ – кількість вузлів в j -му сегменті мережі включно з маршрутизатором; $N_{kn,v,p,z,j} \leq N_{kn,v,p,z}$; $i = 1, 2, \dots, N_{kn,v,p}$; $N_{kn,v,p}$ – кількість підмножин вузлів корпоративних мереж в множині $M_{kn,p}$.

Вектор j – координат X_j задамо з урахуванням формули (3) так:

$$X_j = \begin{pmatrix} x_{kn,v,p,z,vect,1,j} \\ x_{kn,v,p,z,vect,2,j} \\ \dots \\ x_{kn,v,p,z,vect,N_{kn,v,p,j}} \end{pmatrix}, \quad (4)$$

де $x_{kn,v,p,z,vect,i,j}$ – координата на координатній площині компоненти вектору з елементів підмножини $M_{kn,v,p,i}$ ($i = 1, 2, \dots, N_{kn,v,p}$, $N_{kn,v,p}$ – кількість підмножин вузлів корпоративних мереж в множині $M_{kn,p}$); $N_{kn,v,p,z}$ – максимальна кількість вузлів в сегментах мережі включно з маршрутизатором; j – номер стовпця матриці; $j = 1, 2, \dots, N_{kn,v,p,z,N_{kn,v,p,z,j}}$; $j = 1, 2, \dots, N_{kn,v,p,z,j}$; $N_{kn,v,p,z,j}$ – кількість вузлів в j -му сегменті мережі включно з маршрутизатором; $N_{kn,v,p,z,j} \leq N_{kn,v,p,z}$; $i = 1, 2, \dots, N_{kn,v,p}$; $N_{kn,v,p}$ – кількість підмножин вузлів корпоративних мереж в множині $M_{kn,p}$.

Множина K_{os} може містити такі елементи:

- 1) $k_{kod,1}$ – комп'ютерні станції з компоненти обманних систем, але не містять приманок чи пасток;
- 2) $k_{kod,2}$ – комп'ютерні станції з компоненти обманних систем і містять приманки та/чи пастки;
- 3) $k_{kod,3}$ – комп'ютерні станції приманок та/чи пасток;
- 4) $k_{kod,4}$ – маршрутизатори;
- 5) $k_{kod,5}$ – сервери з компоненти обманних систем, але не містять приманок чи пасток;
- 6) $k_{kod,6}$ – сервери з компоненти обманних систем і містять приманки та/чи пастки.

Об'єкти корпоративних мереж $k_{kod,1} - k_{kod,6}$ можуть бути поділені на такі що перебувають в демілітаризованій зоні і такі, що не знаходяться в ній. А також можуть об'єкти поділені за територіальним принципом, тобто якщо вони знаходяться в різних будівлях чи приміщеннях, включно на приватній території. Тоді, кількість таких об'єктів збільшується. До них також можуть відноситись IP-камери.

Побудуємо один з варіантів функції $F_{os,kod}$ (формула (3)). Нехай n_R – кількість об'єктів корпоративних мереж в R – сегменті, причому R також буде номером сегменту, а на координатній площині буде значенням радіусу кола. Якщо в корпоративній мережі є один радіус кола, тоді він дорівнює одиниці $R = 1$ і це буде означати відсутність поділу на сегменти, тобто наявність всіх вузлів корпоративної мережі в одному сегменті. Якщо буде два сегменти, то кіл на координатній площині буде два з радіусами $R = 1$ та $R = 2$. Аналогічно, можна узагальнити таке представлення для довільної кількості сегментів в корпоративних мережах. Тоді, для такого випадку буде кількість кіл така як і кількість сегментів, а радіус кіл буде обиратись з послідовності чисел $R = 1, 2, 3, \dots, k_R$, де k_R – кількість сегментів.

Розмістимо об'єкти корпоративних мереж одного сегменту на колі у вершинах правильного багатокутника, який вписано в це коло. Можливі варіанти вибору довільного багатокутника, але тоді потрібно задати функцію, яка встановлює відстані на колі між двома точками, і для всіх точок ця функція має коректно встановлювати координати. У випадку вибору правильного багатокутника всі сусідні точки на колі будуть рівновіддалені. Для знаходження координат n -кутника, який вписаний в коло з радіусом R та центром в точці $O(0;0)$ координатної площини, задамо початкову вершину від якої будуть визначатись координати всіх решти вершин на колі. Для того, щоб при наявності двох і більше кіл початкові точки не були на одній півосі задамо координати початкових точок з врахуванням їх зміщення та в залежності від номерів кіл, які визначаються різними за довжиною радіусами. Координати початкових точок з урахуванням довжин радіусів на координатній площині:

$$\begin{aligned} x_{1,R_m} &= R_m * \cos(m^\circ); \\ x_{2,R_m} &= R_m * \sin(m^\circ); \\ R_m &= m; m \in N; m = 1, 2, 3, \dots, \end{aligned} \quad (5)$$

де m – натуральне число, що змінюється від одиниці до значення кількості сегментів корпоративної мережі; R_m – радіус кола з початком в центрі координат; $(x_{1,R_m}; x_{2,R_m})$ – координати початкової точки багатокутника на координатній площині.

Кут зміщення кожної наступної початкової вершини багатокутника на кожному наступному колі збільшується на 1° .

Перевірку правильності заданих координат початкових точок багатокутників здійснимо обчисленням довжини радіуса між центром координатної площини і отриманими за формулою (5) координатами точок здійснимо згідно формули рівняння кола:

$$(x_{1,R_m})^2 + (x_{2,R_m})^2 = R_m^2. \quad (6)$$

Перша початкова точка на колі для багатокутника буде знаходитись на осі абсцис і її значення $x_{1,R_1} = 1$, $x_{2,R_1} = 0$. Друга початкова точка - $x_{1,R_2} = 2 * \cos(2^\circ)$, $x_{2,R_2} = 2 * \sin(2^\circ)$, третя початкова точка - $x_{1,R_3} = 3 * \cos(3^\circ)$, $x_{2,R_3} = 3 * \sin(3^\circ)$.

Правильні багатокутники, які вписані в кола, будуть мати різну кількість вершин, але частина з них може мати однакову кількість вершин. При цьому вони будуть мати різні розміри, бо радіуси кіл для них різні, та їх початкові точки і решта відповідних за номерами точок не будуть належати відповідним прямим, які проходять через центр кола через зміщення координат початкових точок для кожного багатокутника.

Фактично згідно формули (5) позначення точок для визначення їх значень буде таким:

$$x_{kn,v,p,z,vect,R_m,1} = x_{1,R_m}; x_{kn,v,p,z,vect,R_m,2} = x_{2,R_m}. \quad (7)$$

Решту вершин з їх координатами отримуємо, обертаючи початкову вершину на кут, що дорівнює $\frac{360^\circ}{n_{R_m}}$, де n_{R_m} – кількість об'єктів в сегменті корпоративних мереж. Якщо в сегменті знаходиться один об'єкт, тоді він розміщується в початкову точку багатокутника відповідного кола. Координати решти точок на колах, які є вершинами n_{R_m} - кутників визначаємо так:

$$x_{1,R_m} = R_m * \cos\left(m^\circ + (n_{R_m} - 1) * \frac{360^\circ}{n_{R_m}}\right); x_{2,R_m} = R_m * \sin\left(m^\circ + (n_{R_m} - 1) * \frac{360^\circ}{n_{R_m}}\right); \quad (8)$$

$$R_m = m; m \in N; m = 1, 2, 3, \dots; n_{R_m} \in N; n_{R_m} = 1, 2, 3, \dots$$

Таким чином, підготовчий етап для імплементації алгоритму молі і полум'я полягає у поданні об'єктів корпоративних мереж на координатній площині з поділом їх між сегментами. Таке подання є необхідним для забезпечення керування обманими системами приманками і пастками в контексті оптимізації частини кроків систем під час КА чи дій ЗПЗ та співвіднесення їх до місць впливів КА та дій ЗПЗ. Геометричну інтерпретацію такого подання, в якому використано формули (5) та (8), та прикладу потенційної спіралі зображено на рис. 2.

Аналогічно, для тримірного та багатомірного просторів можна також задати формулами координати точок в просторі, причому для тримірного простору об'єкти корпоративних мереж будуть розміщені на сферах, які будуть мати один центр і вкладатись одна в одну, а спіраль буде лінією в просторі, а не в площині.

Геометрична інтерпретація розміщення об'єктів корпоративних мереж в сегментах та потенційної спіралі на рис. 2 може бути модифікована таким чином, що кожне коло буде в окремій паралельній площині. Тоді, спіраль також буде розташована в тримірному просторі, а не в площині.

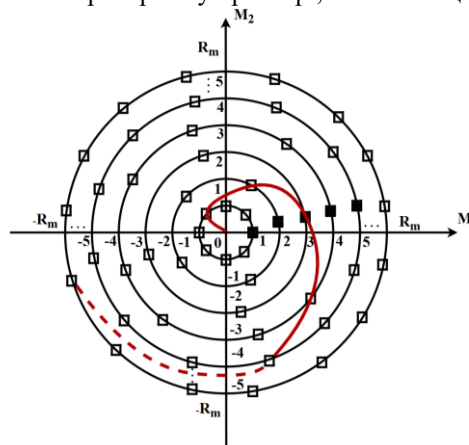


Рис. 2. Геометрична інтерпретація розміщення об'єктів корпоративних мереж в сегментах та сліду потенційної спіралі

Функція для розміщення об'єктів корпоративних мереж є дискретною величиною, перелік наступних кроків обманих є дискретною величиною, тому будемо здійснювати дискретну оптимізацію алгоритмом молі і полум'я.

На наступному етапі, після підготовчого етапу, задамо об'єкти, на які здійснюються впливи КА та дій ЗПЗ, а також компоненти обманих систем та приманки і пастки з урахуванням рис. 2 та формул (3)-(5), (7).

Розглянемо спочатку пряму схему, в якій в центрі системи координат знаходиться приманка та/або пастка, а в об'єктах корпоративних мереж, які розміщені на колах, відображено впливи КА чи дій ЗПЗ, причому ці впливи можуть бути не в усіх об'єктах корпоративних мереж. ЗПЗ може активним в певних вузлах корпоративних мереж і, тоді, такі вузли будемо вважати об'єктами, в яких наявні міль. Аналогічно, об'єкти на які спрямовані КА та на них відбуваються певні впливи теж вважатимемо такими, що в них може бути міль. А у випадку отримання контролю над об'єктами корпоративних мереж під час КА в них зловмисник втілює ЗПЗ для здійснення контролю над ними або здійснює знищення всього що в ньому наявне, то цей варіант будемо розглядати теж як наявність молі, що відповідатиме першим двом із наявним вже ЗПЗ та впливами КА. Таким чином, КА чи дії ЗПЗ, а також саме ЗПЗ, спрямовані чи наявні в об'єктах корпоративних мереж будемо позиціонувати як міль. Тобто, припускаємо, що кандидатами в контексті розв'язків є моль і її може бути більше однієї, а змінними задачі є положення молі у просторі. Тоді, моль, якої більше однієї, можуть лігати в просторі будь-якого виміру зі змінною векторів свого положення. Таким об'єктам на координатній площині призначимо певний колір і задамо їх матрицею координат у певному вимірному просторі так:

$$A_M = \begin{pmatrix} a_{1,1} & \dots & a_{1,N_{A_M,s}} \\ \vdots & \ddots & \vdots \\ a_{N_{A_M,r},1} & \dots & a_{N_{A_M,r},N_{A_M,s}} \end{pmatrix}, \quad (9)$$

де $a_{i,j}$ – координата молі у певному вимірному просторі; $N_{A_{M,S}}$ – розмірність простору; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; $j = 1, 2, 3, \dots, N_{A_{M,S}}$.

В поданні матрицею A_M сформовано популяцію метеликів молі в поточний момент часу. Через певний проміжок часу вона може змінитись кількісно. Для формул (5) та (8) і зображенню на рис. 2 значення $N_{A_{M,S}} = 2$.

Вплив, переміщення та перебування КА чи дій ЗПЗ в об'єктах корпоративних мереж є основою для визначення подальших кроків обманних систем. Серед цих об'єктів можуть бути і хибні об'єкти для атак, але керування ними здійснюють обманні системи. При цьому можна оцінити вплив, переміщення чи перебування КА чи дій ЗПЗ в об'єктах корпоративних мереж і для такого оцінювання введемо функцію допасованості, яка буде відображати близькість конструктивного рішення до поставленої цілі. Таке значення функції допасованості будемо визначати для кожної молі за її координатами, що задані за формулою (9) і тоді отримаємо таку матрицю:

$$F_1^{A_M} = \begin{pmatrix} F_{1,1}^{A_M} \\ F_{1,2}^{A_M} \\ \dots \\ F_{1,N_{A_{M,r}}}^{A_M} \end{pmatrix}, \quad (10)$$

де $F_{1,j}^{A_M}$ – значення функції допасованості $F_1^{A_M}$ для j -тої молі; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; $j = 1, 2, 3, \dots, N_{A_{M,S}}$.

Приманки і пастки можуть бути розміщені в просторі і визначатись координатами. В центрі координат може бути приманка чи пастка до якої прагне наблизитись моль, але приманки і пастки можуть бути не активними і перебувати на шляху молі. Задамо полум'я, що відповідатиме приманкам і пасткам, а також компонентам обманних систем, матрицею B_M аналогічно до матриці A_M так:

$$B_M = \begin{pmatrix} b_{1,1} & \dots & b_{1,N_{A_{M,S}}} \\ \vdots & \ddots & \vdots \\ b_{N_{A_{M,r}},1} & \dots & b_{N_{A_{M,r}},N_{A_{M,S}}} \end{pmatrix}, \quad (11)$$

де $b_{i,j}$ – координата полум'я у певному вимірному просторі; $N_{A_{M,S}}$ – розмірність простору; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявне полум'я; $j = 1, 2, 3, \dots, N_{A_{M,S}}$.

Прийmemo розмірності матриць A_M і B_M однаковими виходячи з того, що метелики молі є пошуковими агентами, які переміщуються в просторі пошуку, а полум'я є їх найкращою позицією в поточний момент часу. В контексті покращення функціонування обманних систем та дискретної оптимізації однакові розмірності матриць підходять для КА чи дій ЗПЗ, коли для протидії їм здійснюється підбір відповідних засобів і їх кількість залежить від виявлених зловмисних впливів, що є кроками обманних систем, та в загальному підборі кроків з множини кроків систем. Тобто, полум'я можна розглядати орієнтиром для молі в просторі пошуку. Тоді, міль здійснює пошук навколо полум'я і оновлює його при знаходженні кращого рішення. Тому, внаслідок таких цілеспрямованих дій вона ніколи не втрачає свого найкращого рішення. Для КА чи дій ЗПЗ відбуваються спрямування на об'єкти, які є метою зловмисників. В цьому процесі наближення до мети покращує наступні варіанти. Зі сторони обманних систем теж наявне спрямування на опрацювання зловмисних впливів, яке досягається долученням нових приманок і пасток, що відображається певними кроками систем і, при цьому, вибір кроків здійснюється з уточненням стану в середовищах корпоративних мереж, тобто на кожному етапі обирається кращий варіант кроків. Введемо аналогічно до функції допасованості $F_1^{A_M}$ функцію допасованості $F_2^{B_M}$ для оцінювання варіантів з матриці B_M так:

$$F_2^{B_M} = \begin{pmatrix} F_{2,1}^{B_M} \\ F_{2,2}^{B_M} \\ \dots \\ F_{2,N_{A_{M,r}}}^{B_M} \end{pmatrix}, \quad (12)$$

де $F_{2,j}^{B_M}$ – значення функції допасованості $F_2^{B_M}$ для j -того полум'я; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявне полум'я; $j = 1, 2, 3, \dots, N_{A_{M,S}}$.

Розглянемо кроки алгоритму дискретної оптимізації молі і полум'я, за яким здійснюється апроксимація глобального оптимуму.

Задаємо три функції формулами (13)-(15) згідно стандартного підходу з роботи [7].

Функція F_1^A генерує випадкову популяцію молі, розміщує її у просторі, тобто формує матрицю A_M (формула (9)), та обчислює значення функції допасованості $F_1^{A_M}$ (формула (10)) для згенерованої популяції

молі і задамо її так:

$$F_1^A: \emptyset \rightarrow \{A_M, F_1^{AM}\}. \quad (13)$$

Функція F_2^A є основною функцією. Вона переміщує міль у просторі пошуку. Ця функція після отримання матриці A_M повертає її з оновленими значеннями елементів, тобто після її виконання знову отримуємо матрицю A_M . Задамо функцію F_2^A так:

$$F_2^A: A_M \rightarrow A_M. \quad (14)$$

Функція F_3^A повертає значення «істинне», якщо критерій завершення алгоритму задовольняється, і значення «хибне», якщо критерій завершення не задовольняється.

Задамо функцію F_3^A так:

$$F_3^A: A_M \rightarrow \{true, false\}. \quad (15)$$

Згідно введених визначимо алгоритм дискретної оптимізації молі і полум'я так:

$$\begin{aligned} A_M &= F_1^A(); \\ \text{поки } F_3^A(A_M) &= \{false\} \\ A_M &= F_2^A(A_M); \end{aligned} \quad (16)$$

кінець

Функція F_1^A повинна генерувати початкові рішення та обчислювати значення цільової функції F_1^{AM} , яку задано за формулою (10). У функції F_1^A можна використовувати будь-який випадковий розподіл. Задамо такий розподіл:

$$\begin{aligned} \text{для } i &= 1, n; \text{ крок } 1 \\ \text{для } i &= 1, n; \text{ крок } 1 \\ a_{i,j} &= (c_i - d_i) * rand() + d_i; \end{aligned} \quad (17)$$

кінець

кінець

$$F_1^{AM} = F_1^{AM}(A_M);$$

де $a_{i,j} \in A_M$; $a_{i,j}$ – координата молі у певному вимірному просторі; $N_{AM,s}$ – розмірність простору; $i = 1, 2, 3, \dots, N_{AM,r}$; $N_{AM,r}$ – кількість об'єктів, в яких наявна міль; $j = 1, 2, 3, \dots, N_{AM,s}$.

Для попереднього алгоритму матриці C та D , елементи яких визначають верхню і нижню межі зміни значень, задамо їх елементами так:

$$C = (c_1, c_2, \dots, c_{N_{AM,r}}); D = (d_1, d_2, \dots, d_{N_{AM,r}}), \quad (18)$$

де елементи матриці C є значеннями верхньої межі i -тої змінної; елементи матриці D є значеннями нижньої межі i -тої змінної; c_i – елемент матриці C ; d_i – елемент матриці D ; $i = 1, 2, 3, \dots, N_{AM,r}$; $N_{AM,r}$ – кількість об'єктів, в яких наявна міль.

Функція F_2^A виконується ітеративно і переміщує моль в просторі пошуку. Після повернення значення $\{true\}$ функцією F_3^A її виконання завершиться. Простір пошуку є дискретним і визначається матрицею векторів $M_{kn,v,p,z,vect}$ та матрицею A_M (формула (9)). Він відображається на координатній площині на рис.2.

Алгоритм дискретної оптимізації молі і полум'я характеризується особливістю, яка полягає в дотриманні поперечної орієнтації при здійсненні вибору наступного положення молі щодо полум'я. Задамо такий рух так:

$$A_{M,i} = Q(A_{M,i}, B_{M,i}), \quad (19)$$

де $\bigcup_{i=1}^{N_{AM,r}} A_{M,i} = A_M$; $A_{M,i}$ – i – та моль; $\bigcup_{i=1}^{N_{AM,r}} B_{M,i} = B_M$; $A_{M,i}$ – i – та приманка чи пастка або компонента обманної системи; $i = 1, 2, 3, \dots, N_{AM,r}$; $N_{AM,r}$ – кількість об'єктів, в яких наявна міль; Q – функція, яка задаватиме поперечну орієнтацію при здійсненні вибору наступного положення молі щодо полум'я.

Функція Q буде визначати рух. Оскільки завдання з вибору кроків належить до дискретної оптимізації і побудоване пошукове поле теж є дискретним, то функція Q буде дискретною. Спіраль є основою схемою, згідно якої має відбуватись оновлення молі. Варіантів спіралей може бути багато і задаватись вони можуть різними варіантами функції Q . Але необхідне виконання таких умов при конструюванні варіантів функції Q :

- 1) рух повинен бути по спіралі;
- 2) рух повинен виконуватись винятково з дотриманням поперечної орієнтації;

3) початкова гранична точка спіралі повинна бути в одному з об'єктів корпоративних мереж, в якому встановлені потенційно зловмисні прояви, або в загальному підході – з точки чи кроку, в яких розпочато процес;

4) фінальною граничною точкою спіралі повинна бути точка з полум'ям;

5) відхилення спіралі не повинно виходити за межі пошукового простору, тобто спіраль повинна перебувати в межах крайніх точок, які максимально віддалені від центру (від точки з полум'ям);

6) спіраль не повинна вироджуватись у відрізок, що сполучає граничні точки по прямій лінії;

7) спіраль не повинна містити зворотні дуги і бути спрямована або за годинниковою стрілкою або проти годинниковою стрілки;

8) побудова спіралі повинна узгоджуватись з часом як параметром;

9) полум'я з часом може змінювати свої координати;

10) кожна наступна дуга між обраними для спіралі кроками повинна бути на тому ж колі, що й попередня дуга, або ближче до полум'я;

11) при оновленні місця полум'я оновлюються координати молі;

12) при наявності більше однієї молі та одного полум'я діє вимога, що моль, яка є першою серед всіх, повинна наближатись до полум'я раніше решти;

13) при наявності більше однієї молі та одного полум'я діє вимога, що моль, яка є останньою серед всіх, отримує розв'язок з решти, які залишились;

14) при наявності більше одного полум'я і більше однієї молі, але при їх однаковій кількості, рух кожної молі спрямовується до окремого полум'я і кількість полум'я зменшується з часом;

15) при наявності більше одного полум'я і більше однієї молі, але при їх різній кількості, рух кожної молі прагне до окремого полум'я, але за відсутності достатньої кількості полум'я розподіляється між ними, і кількість полум'я зменшується з часом.

Для конструювання функції Q згідно визначених умов введемо такі правила:

1) $\forall x_{l,i}: x_{l,i+1} \leq x_{l,i}$; l – кількість координат; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль;

2) $\forall x_{l,i}: x_{l,i+1} = x_{l,i}$ або $x_{l,i+1} < x_{l,i}$; l – кількість координат; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль;

3) a_1 (координати в матриці A_M , яку задано формулою (9)) міститься в одному з елементів матриці $M_{kn,v,p,z,vec}$; $a_{i,j}$ – координата молі a_1 у певному вимірному просторі; $N_{A_{M,s}}$ – розмірність простору; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; $j = 1, 2, 3, \dots, N_{A_{M,s}}$;

4) $a_{N_{A_{M,r}}}$ (координати в матриці A_M , яку задано формулою (9)) міститься в одному з елементів матриці $M_{kn,v,p,z,vec}$; $a_{i,j}$ – координата молі a_1 у певному вимірному просторі; $N_{A_{M,s}}$ – розмірність простору; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; $j = 1, 2, 3, \dots, N_{A_{M,s}}$;

5) $\forall x_{l,i}: (x_{l,1,R_l})^2 + (x_{l,2,R_l})^2 \leq R_{max}^2$; l – кількість координат; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; R_{max} – радіус найбільшого кола;

6) $\exists a_s: a_s \in$ спіралі $[a_1; a_{N_{A_{M,r}}}]$, тобто між крайніми точками наявна мінімум одна точка;

7) якщо спіраль сформовано проти руху годинникової стрілки, тоді кут повороту спіралі $\varphi > 0$ та не може бути від'ємним; якщо навпаки – спіраль сформовано за рухом годинникової стрілки, тоді кут повороту спіралі $\varphi < 0$ та не може бути додатнім;

8) якщо t_1 – час, протягом якого обманна система підтримує дії та визначає кроки в межах однієї системи координат (рис. 3.3), тоді $t_0 = 0$ і $\lim_{t=t_1, t_2, t_3, \dots, t_p, t_0} t = 0$ (p – номер передостанньої ітерації визначення часу), $t_1 > t_2 > t_3 > \dots > t_p > t_0$;

9) оновлення матриці B_M (формула (11)) з урахуванням вимоги п. 5;

10) $\forall x_{l,i}, x_{l+1,i}: (x_{l,1,R_s})^2 + (x_{l,2,R_s})^2 \leq R_s^2$; $(x_{l+1,1,R_{s-1}})^2 + (x_{l+1,2,R_{s-1}})^2 \leq R_{s-1}^2$; l – кількість координат; $i = 1, 2, 3, \dots, N_{A_{M,r}}$; $N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль; R_s – радіус більшого кола; R_{s-1} – радіус меншого кола; $[x_{l,i}; x_{l+1,i}]$ – дуга спіралі;

11) оновлення матриці A_M (формула (9)) з урахуванням вимоги п. 9;

12) якщо матриця A_M (формула (9)) більше одного рядка, тобто більше однієї молі, тоді прийнявши верхні рядки матриці за такі, що відповідають першим в послідовності молі, а нижні рядки – останнім, тобто послідовність молі сформовано за номерами $i = 1, 2, 3, \dots, N_{A_{M,r}}$ ($N_{A_{M,r}}$ – кількість об'єктів, в яких наявна міль) від першої до останньої, то різниця відстаней з врахуванням координат з матриці A_M кожної молі і координатами центру буде формувати зростаючу послідовність;

13) якщо матриця A_M (формула (9)) більше одного рядка, то кількість розв'язків для послідовності молі зменшується від першої до останньої, які задано за номерами $i = 1, 2, 3, \dots, N_{A_M, r}$ ($N_{A_M, r}$ – кількість об'єктів, в яких наявна міль) від першої до останньої;

14) оновлення матриці B_M (формула (11)) з поділом її на дві матриці і більше;

15) оновлення матриці B_M (формула (11)) з поділом її на дві матриці і більше та оновлення матриці A_M (формула (9)).

Введені правила 1-15 відповідають алгоритму дискретної оптимізації молі і полум'я та дають змогу сформувати варіанти кроків, або вузлів, зокрема і з приманками і пастками, в які може переміститись міль в процесі руху по спіралі. Таких кроків може бути декілька.

Враховуючи правила 1-15 задамо функцію Q так:

$$Q(a_k) = \begin{cases} \varphi = \varphi + \theta, \text{ якщо } M_k = \emptyset; \text{ інакше} \\ m_s, \text{ якщо } M_k \neq \emptyset \text{ та } \min_{M_k} F_{os}(v_{os, i}, v_{os, i, u}) \end{cases}, \quad (20)$$

де $m_s \in M_k$; F_{os} – цільова функція оцінювання обраних варіантів (формула (3.2)); $v_{os, i, u, j}$ – крок обманної системи з приманками і пастками; $j = 1, 2, \dots, N_{os, i, u}$; $N_{os, i, u}$ – кількість кроків обманних систем з приманками і пастками для вирішення певного завдання, які визначено системою в поточний момент часу; i – i -та послідовність кроків для вирішення певного завдання системи; u – уточнення кроків, які задано вектором $v_{os, i}$.

Основні кроки методу синтезу популяційних алгоритмів в архітектурі обманних систем з приманками і пастками:

1) підготовка даних та їх кодування для формування дискретного простору пошуку (формули (1)-(8), рис. 2);

2) формування матриць молі та полум'я і відповідні їм функції допасованості (формули (9)-(12));

3) введення величини час до дискретного простору пошуку (рис. 3);

4) задамо три функції (формули (13)-(15)) для реалізації алгоритму дискретної оптимізації молі і полум'я;

5) згідно введених функцій з п. 4 за формулами (16)-(18) виконуємо кроки алгоритму дискретної оптимізації молі і полум'я;

6) виконуємо правила 1-15 та знаходимо значення функції Q (формула (20)) для формування варіантів кроків згідно заданого кута для сектора із значеннями;

7) задаємо та відображаємо рух по спіралі за формулою (19).

Основні сім кроків методу не є чітко детерміновані в контексті послідовного виконання. Частина з кроків, крім кроку 1, можуть виконуватись паралельно або багатократно, тобто будуть викликатись з певних інших кроків.

Таким чином, здійснено синтез алгоритму комбінаторної оптимізації молі і полум'я в архітектурі обманних систем з приманками і пастками в корпоративних мережах, особливістю якого є формування дискретного простору пошуку з поданням об'єктів координатами у вимірних просторах, синтез спіралі в дискретному просторі пошуку на основі оцінювання потенційних варіантів наступних кроків та множини елементів у визначеному секторі, врахування часу в контексті вибору кроків, забезпечення зміни розташування полум'я та молі, що дало змогу забезпечити вибір та зміну кроків для функціонування обманних систем з приманками і пастками протягом тривалого часу під час КА чи дій ЗПЗ для заплутування злоумисників.

Слід спіралі поєднує об'єкти в дискретному просторі пошуку. Він відображає рух молі до полум'я, що відповідає саме алгоритму молі і полум'я, та ним задано необхідні кроки із формування сліду спіралі та зміни позицій молі і полум'я. Також в алгоритмі враховано час як параметр, що дає змогу фіксувати побудову сліду спіралі і, відповідно, зміну кроків системою. Досліджено формування сліду спіралі на основі величини кута для сектору, в якому знаходяться наступні кроки систем, та визначено правила для формування сегментів спіралі. Для уникнення швидкої збіжності в локальному оптимумі в алгоритмі дискретної оптимізації молі і полум'я задані кроки з оновлення розміщення полум'я і молі, що дає змогу перебувати молі тривалий час навколо полум'я і обирати варіанти кроків з глобального оптимуму. Поперечна орієнтація, як ознака цього алгоритму натхненню природою, забезпечена рухом молі по дотичній до одного кола або перехід її в нове положення в колі меншого радіуса за попереднє коло. При наявності більше однієї молі перша моль обирає кращі варіанти, а наступні молюбирають з тих, варіантів, які залишаються. Таким чином, остання моль обирає за залишковим принципом. Це дає змогу в подальшому сортувати їх за ступенем допасованості і оцінювати доцільність переміщення полум'я в дискретному просторі пошуку.

Розроблений метод синтезу популяційних алгоритмів в архітектурі обманних систем з приманками і пастками дає змогу створювати обманні системи для заплутування злоумисників в корпоративних мережах.

РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТУ

Результати роботи розробленої обманної системи з приманками і пастками протягом тривалого періоду (90 діб) функціонування в корпоративних мережах з урахуванням здійснення симуляцій комп'ютерних атак різного типу, зокрема і відмови в обслуговуванні подано в табл. 1 з потенційним полем подій при проведенні зловмисниками двоцільових атак.

Таблиця 1

Поле подій та результати					
№ з/п	Варіанти подій	1*	2*	3*	4*
1	КА чи ЗПЗ завершилися в приманках чи пастках;	67	62	6	11
2	КА чи ЗПЗ потрапили в приманки чи пастки, але при цьому їх активність продовжилася на інших напрямках;	8	17	2	2
3	КА чи ЗПЗ надали змогу зловмисникам отримати контроль над приманками чи пастками, з якими увійшли в контакт	4	3	1	3
4	КА чи ЗПЗ досягли мети зловмисників і не були помічені обманними системами з приманками і пастками	17	12	0	1
5	КА чи ЗПЗ не досягли мети зловмисників і не були помічені обманними системами з приманками і пастками	4	6	0	1
Разом:		100	100	9	18

Позначення:

1* - зловмисник здійснив одну двоцільову КА;

2* - зловмисник здійснив більше однієї різних двоцільових КА;

3* - ЗПЗ здійснило поширення в одній комп'ютерній станції;

4* - ЗПЗ здійснило поширення в багатьох комп'ютерних станціях.

Обманна система згідно результатів експерименту, які подано в табл. 1, адекватно реагувала на КА чи дії ЗПЗ, що підтверджено відсотком правильних спрацювань.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ

І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Таким чином, розроблено метод синтезу алгоритму дискретної оптимізації молі й полум'я, адаптований для архітектури обманних систем із приманками та пастками. Запропонований підхід забезпечує формування координатного дискретного простору пошуку та створення динамічного спірального сліду, що дозволяє уникнути передчасної збіжності до локальних оптимумів. Розв'язання задачі вибору наступних кроків обманної системи в умовах змінних параметрів корпоративного середовища розглядається як оптимізаційна проблема, спрямована на підвищення ефективності виявлення кіберзагроз.

Метод дає змогу знаходити адаптивну оптимальну послідовність кроків реагування на дії зловмисника, що сприяє створенню обманних систем із підвищеною автономністю, стійкістю до розкриття принципів їх роботи та мінімальною потребою в участі адміністратора. Експериментальні результати підтверджують ефективність і перспективність використання популяційних алгоритмів у цьому контексті.

Подальші дослідження мають бути спрямовані на глибшу інтеграцію популяційних методів в архітектуру обманних систем та розроблення механізмів їхнього функціонування відповідно до запропонованої концептуальної моделі. Отримані результати сприяють підвищенню рівня кіберзахисту корпоративних мереж завдяки створенню інтелектуальних адаптивних засобів протидії сучасним атакам і зловмисному ПЗ.

Література

1. Kashtalian, A., Lysenko, S., Kysil, T., Sachenko, A., Savenko, O., & Savenko, B. Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*. 2025. Vol. 24(1), 35-51. DOI: <https://doi.org/10.47839/ijc.24.1.3875>
2. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 265-270, doi: <https://doi.org/10.1109/IDAACS58523.2023.10348773>
3. Kashtalian, A., Lysenko, S., Sachenko, A., Savenko, B., Savenko, O., & Nicheporuk, A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*. 2025. Vol. 1. Pp. 264-297. DOI: <https://doi.org/10.32620/reks.2025.1.18>
4. Kashtalian A., Savenko O., Sachenko A. Agglomerative clustering of data collected by honeypots. 2021 11th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), Cracow, Poland, 22–25 September 2021. 2021. DOI: <https://doi.org/10.1109/idaacs53288.2021.9661027>

5. Kashtalian A., Sochor T. K-Means clustering of honeynet data with unsupervised representation learning. International workshop on intelligent information technologies & systems of information security. *CEUR workshop proceedings*. Vol. 2853. 2021. P. 539–549. URL: <https://ceur-ws.org/Vol-2853/paper48.pdf>
6. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024. Vol. 1. Pp. 152–175. DOI: <https://doi.org/10.32620/reks.2024.1.13>
7. Mirjalili S. Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. *Knowledge-Based Systems* (2015), DOI: <http://dx.doi.org/10.1016/j.knosys.2015.07.006>
8. Rotshtein A.P., Zelinska O.V., Kaminskyi V.P. Optimization of Product Quality Indicators in the “Producer–Consumer” System Based on Fuzzy Cognitive Maps and Genetic Algorithm. *Cybern Syst Anal*. 2024. Vol. 60. Pp. 600–612. DOI: <https://doi.org/10.1007/s10559-024-00699-y>
9. Штовба С. Д. Генетичний алгоритм вибору правил нечіткої бази знань, збалансованої за критеріями точності та компактності [Електронний ресурс] / С. Д. Штовба, В. В. Мазуренко, Д. А. Савчук // *Наукові праці Вінницького національного технічного університету*. – 2012. – № 3. URL : <http://praci.vntu.edu.ua/index.php/praci/article/view/331>
10. Shafronenko A. Y., Bodyanskiy Y. V., Holovin O. O. CLUSTERIZATION OF DATA ARRAYS BASED ON THE MODIFIED GRAY WOLF ALGORITHM . *Radio Electronics, Computer Science, Control*, 2023. Vol. 1, 73. DOI: <https://doi.org/10.15588/1607-3274-2023-1-7>
11. Bodyanskiy, Y. V., Pliss, I. P., & Shafronenko, A. Y. CLUSTERIZATION OF DATA ARRAYS BASED ON COMBINED OPTIMIZATION OF DISTRIBUTION DENSITY FUNCTIONS AND THE EVOLUTIONARY METHOD OF CAT SWARM. *Radio Electronics, Computer Science, Control*, 2021. Vol. 4. 61. DOI: <https://doi.org/10.15588/1607-3274-2022-4-5>
12. Bodyanskiy Y. V., Shafronenko A. Y. , Pliss I. P. Credibilistic fuzzy clustering based on evolutionary method of crazy cats, *System Research and Information Technologies*, 2021 (3), pp. 110–119. DOI: <https://doi.org/10.20535/SRIT.2308-8893.2021.3.09>
13. Прикладні методи комбінаторної оптимізації: навч. посіб. / Л. Ф. Гуляницький, О. Ю. Мулеса. – К. : Видавничо-поліграфічний центр «Київський університет», 2016. – 142 с.
14. Mirjalili S. The ant lion optimizer, *Advances in Engineering Software*, 2015, Vol. 83, pp. 80–98. DOI: <https://doi.org/10.1016/j.advengsoft.2015.01.010>
15. Mirjalili S. M., Lewis A. Grey wolf optimizer, *Advances in Engineering Software*, 2014, Vol. 69, pp. 46–61. DOI: <https://doi.org/10.1016/j.advengsoft.2013.12.007>
16. Povkhan I., Leheza A., Mulesa O., Melnyk O., Kintonova A. Method of hybrid logical classification trees based on group selection of discrete features. *Informatyka, Automatyka, Pomiar W Gospodarce I Ochronie Środowiska*. 2025. № 15(3). Pp. 15–21. DOI: <https://doi.org/10.35784/iapgos.6957>
17. Mulesa, O., & Bohdan, Y. Development of a fuzzy production model for assessing the degree of information security in international cooperation. *Technology Audit and Production Reserves*. 2024. № 6(2(80)). Pp. 6–10. DOI: <https://doi.org/10.15587/2706-5448.2024.318446>
18. Syberfeldt A., Lidberg S. Real-world simulation-based manufacturing optimizations using cuckoo search, *Proceedings of the 2012 Winter Simulation Conference (WSC)*. Berlin, Germany, December 2012, proceedings, pp. 1–12. DOI: <https://doi.org/10.1109/WSC.2012.6465158>
19. Sahoo, S.K., Saha, A.K., Ezugwu, A.E. *et al.* Moth Flame Optimization: Theory, Modifications, Hybridizations, and Applications. *Arch Computat Methods Eng* 30, Pp. 391–426 2023. DOI: <https://doi.org/10.1007/s11831-022-09801-z>
20. Sahoo SK, Saha AK (2022) A hybrid moth flame optimization algorithm for global optimization. *J Bionic Eng*. DOI: <https://doi.org/10.1007/s42235-022-00207-y>
21. Rotshtein A., Shtovba S. Genetic Optimization of Multidimensional Technological Process Reliability. In: Levitin, G. (eds) *Computational Intelligence in Reliability Engineering. Studies in Computational Intelligence*, 2007. Vol 39. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-37368-1_9
22. Shtovba S.D. Ant Algorithms: Theory and Applications. *Program Comput Soft* 2005. Vol. 31. Pp. 167–178. DOI: <https://doi.org/10.1007/s11086-005-0029-1>
23. Wu Y., Chen R., Li C., Zhang L., Dai W. An adaptive sine-cosine moth-flame optimization algorithm for parameter identification of hybrid active power filters in power systems. *IEEE Access* 8:156378–156393. 2020. DOI: <https://doi.org/https://doi.org/10.1109/ACCESS.2020.3005717>
24. Wu Y., Chen R., Li C., Zhang L., Cui Z. Hybrid symbiotic differential evolution moth-flame optimization algorithm for estimating parameters of photovoltaic models. *IEEE Access* 8:156328–156346. 2020. DOI: <https://doi.org/https://doi.org/10.1109/ACCESS.2020.3005711>
25. Zhang Z., Qin H., Yao L., Liu Y., Jiang Z., Feng Z., Ouyang S. Improved multi-objective moth-flame optimization algorithm based on R-domination for cascade reservoirs operation. *J Hydrol* 581:124431. 2020. DOI: <https://doi.org/10.1016/j.jhydrol.2019.124431>

26. Wang M., Chen H., Yang B., Zhao X., Hu L., Cai Z., Huang H., Tong C. Toward an optimal kernel extreme learning machine using a chaotic moth-flame optimization strategy with applications in medical diagnoses. *Neurocomputing* 267:69–84. 2017. DOI: <https://doi.org/10.1016/j.neucom.2017.04.060>
27. Ma L, Wang C, Xie N, Shi M, Ye Y, Wang L (2021) Moth-flame optimization algorithm based on diversity and mutation strategy. *Appl Intell.* <https://doi.org/10.1007/s10489-020-02081-9>
28. Zhao X, Fang Y, Liu L, Li J, Xu M (2020) An improved moth-flame optimization algorithm with orthogonal opposition-based learning and modified position updating mechanism of moths for global optimization problems. *Appl Intell* 50(12):4434–4458. <https://doi.org/10.1007/s10489-020-01793-2>
29. Dabba, A., Tari, A. & Meftali, S. Hybridization of Moth flame optimization algorithm and quantum computing for gene selection in microarray data. *J Ambient Intell Human Comput* 12, 2731–2750 (2021). <https://doi.org/10.1007/s12652-020-02434-9>

References

1. Kashtalian, A., Lysenko, S., Kysil, T., Sachenko, A., Savenko, O., & Savenko, B. Method and Rules for Determining the Next Centralization Option in Multicomputer System Architecture. *International Journal of Computing*. 2025. Vol. 24(1), 35-51. DOI: <https://doi.org/10.47839/ijc.24.1.3875>
2. B. Savenko, A. Kashtalian, S. Lysenko and O. Savenko, "Malware Detection By Distributed Systems with Partial Centralization," 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 265-270, doi: 10.1109/IDAACS58523.2023.10348773
3. Kashtalian, A., Lysenko, S., Sachenko, A., Savenko, B., Savenko, O., & Nicheporuk, A. Evaluation criteria of centralization options in the architecture of multicomputer systems with traps and baits. *Radioelectronic and Computer Systems*. 2025. Vol. 1. Pp. 264-297. DOI: <https://doi.org/10.32620/reks.2025.1.18>
4. Kashtalian A., Savenko O., Sachenko A. Agglomerative clustering of data collected by honeypots. 2021 11th IEEE international conference on intelligent data acquisition and advanced computing systems: technology and applications (IDAACS), Cracow, Poland, 22–25 September 2021. 2021. DOI: <https://doi.org/10.1109/idaacs53288.2021.9661027>
5. Kashtalian A., Sochor T. K-Means clustering of honeynet data with unsupervised representation learning. International workshop on intelligent information technologies & systems of information security. *CEUR workshop proceedings*. Vol. 2853. 2021. P. 539–549. URL: <https://ceur-ws.org/Vol-2853/paper48.pdf>
6. Kashtalian, A., Lysenko, S., Savenko, O., Nicheporuk, A., Sochor, T., & Avsiyevych, V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems*, 2024. Vol. 1. Pp. 152-175. DOI: <https://doi.org/10.32620/reks.2024.1.13>
7. Mirjalili S. Moth-flame optimization algorithm: A novel nature-inspired heuristic paradigm. *Knowledge-Based Systems* (2015), DOI: <http://dx.doi.org/10.1016/j.knsys.2015.07.006>
8. Rotshtein A.P., Zelinska O.V., Kaminskiy V.P. Optimization of Product Quality Indicators in the “Producer–Consumer” System Based on Fuzzy Cognitive Maps and Genetic Algorithm. *Cybern Syst Anal*. 2024. Vol. 60. Pp. 600–612. DOI: <https://doi.org/10.1007/s10559-024-00699-y>
9. Штовба С. Д. Генетичний алгоритм вибору правил нечіткої бази знань, збалансованої за критеріями точності та компактності [Електронний ресурс] / С. Д. Штовба, В. В. Мазуренко, Д. А. Савчук // *Наукові праці Вінницького національного технічного університету*. - 2012. - № 3. URL : <http://praci.vntu.edu.ua/index.php/praci/article/view/331>
10. Shafronenko A. Y., Bodyanskiy Y. V., Holovin O. O. CLUSTERIZATION OF DATA ARRAYS BASED ON THE MODIFIED GRAY WOLF ALGORITHM. *Radio Electronics, Computer Science, Control*, 2023. Vol. 1, 73. DOI: <https://doi.org/10.15588/1607-3274-2023-1-7>
11. Bodyanskiy, Y. V., Pliss, I. P., & Shafronenko, A. Y. CLUSTERIZATION OF DATA ARRAYS BASED ON COMBINED OPTIMIZATION OF DISTRIBUTION DENSITY FUNCTIONS AND THE EVOLUTIONARY METHOD OF CAT SWARM. *Radio Electronics, Computer Science, Control*, 2021. Vol. 4. 61. DOI: <https://doi.org/10.15588/1607-3274-2022-4-5>
12. Bodyanskiy Y. V., Shafronenko A. Y., Pliss I. P. Credibilistic fuzzy clustering based on evolutionary method of crazy cats, *System Research and Information Technologies*, 2021 (3), pp. 110–119. DOI: <https://doi.org/10.20535/SRIT.2308-8893.2021.3.09>
13. Прикладні методи комбінаторної оптимізації: навч. посіб. / Л. Ф. Гуляницький, О. Ю. Мулеса. – К. : Видавничо-поліграфічний центр «Київський університет», 2016. – 142 с.
14. Mirjalili S. The ant lion optimizer, *Advances in Engineering Software*, 2015, Vol. 83, pp. 80–98. DOI: <https://doi.org/10.1016/j.advengsoft.2015.01.010>
15. Mirjalili S. M., Lewis A. Grey wolf optimizer, *Advances in Engineering Software*, 2014, Vol. 69, pp. 46–61. DOI: <https://doi.org/10.1016/j.advengsoft.2013.12.007>
16. Povkhan I., Leheza A., Mulesa O., Melnyk O., Kintonova A. Method of hybrid logical classification trees based on group selection of discrete features. *Informatyka, Automatyka, Pomiar W Gospodarce I Ochronie Środowiska*. 2025. № 15(3). Pp. 15–21. DOI: <https://doi.org/10.35784/iapgos.6957>
17. Mulesa, O., & Bohdan, Y. Development of a fuzzy production model for assessing the degree of information security in international cooperation. *Technology Audit and Production Reserves*. 2024. № 6(2(80)). Pp. 6–10. DOI: <https://doi.org/10.15587/2706-5448.2024.318446>
18. Syberfeldt A., Lidberg S. Real-world simulation-based manufacturing optimizations using cuckoo search, *Proceedings of the 2012 Winter Simulation Conference (WSC)*. Berlin, Germany, December 2012, proceedings, pp. 1–12. DOI: <https://doi.org/10.1109/WSC.2012.6465158>
19. Sahoo, S.K., Saha, A.K., Ezugwu, A.E. et al. Moth Flame Optimization: Theory, Modifications, Hybridizations, and Applications. *Arch Computat Methods Eng* 30, Pp. 391–426 2023. DOI: <https://doi.org/10.1007/s11831-022-09801-z>
20. Sahoo SK, Saha AK (2022) A hybrid moth flame optimization algorithm for global optimization. *J Bionic Eng*. DOI: <https://doi.org/10.1007/s42235-022-00207-y>
21. Rotshtein A., Shtovba S. Genetic Optimization of Multidimensional Technological Process Reliability. In: *Levitin, G. (eds) Computational Intelligence in Reliability Engineering. Studies in Computational Intelligence*, 2007. Vol 39. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-37368-1_9
22. Shtovba S.D. Ant Algorithms: Theory and Applications. *Program Comput Soft* 2005. Vol. 31. Pp. 167–178. DOI: <https://doi.org/10.1007/s11086-005-0029-1>
23. Wu Y., Chen R., Li C., Zhang L., Dai W. An adaptive sine-cosine moth-flame optimization algorithm for parameter identification of hybrid active power filters in power systems. *IEEE Access* 8:156378–156393. 2020. DOI: <https://doi.org/https://doi.org/10.1109/ACCESS.2020.3005717>

-
24. Wu Y., Chen R., Li C., Zhang L., Cui Z. Hybrid symbiotic differential evolution moth-flame optimization algorithm for estimating parameters of photovoltaic models. *IEEE Access* 8:156328–156346. 2020. DOI: <https://doi.org/10.1109/ACCESS.2020.3005711>
25. Zhang Z., Qin H., Yao L., Liu Y., Jiang Z., Feng Z., Ouyang S. Improved multi-objective moth-flame optimization algorithm based on R-domination for cascade reservoirs operation. *J Hydrol* 581:124431. 2020. DOI: <https://doi.org/10.1016/j.jhydrol.2019.124431>
26. Wang M., Chen H., Yang B., Zhao X., Hu L., Cai Z., Huang H., Tong C. Toward an optimal kernel extreme learning machine using a chaotic moth-flame optimization strategy with applications in medical diagnoses. *Neurocomputing* 267:69–84. 2017. DOI: <https://doi.org/10.1016/j.neucom.2017.04.060>
27. Ma L., Wang C., Xie N., Shi M., Ye Y., Wang L (2021) Moth-flame optimization algorithm based on diversity and mutation strategy. *Appl Intell.* <https://doi.org/10.1007/s10489-020-02081-9>
28. Zhao X., Fang Y., Liu L., Li J., Xu M (2020) An improved moth-flame optimization algorithm with orthogonal opposition-based learning and modified position updating mechanism of moths for global optimization problems. *Appl Intell* 50(12):4434–4458. <https://doi.org/10.1007/s10489-020-01793-2>
29. Dabba, A., Tari, A. & Meftali, S. Hybridization of Moth flame optimization algorithm and quantum computing for gene selection in microarray data. *J Ambient Intell Human Comput* 12, 2731–2750 (2021). <https://doi.org/10.1007/s12652-020-02434-9>