https://doi.org/10.31891/2307-5732-2025-359-135
УДК 004.75:004.49:004.3

ДРОЗД АНДРІЙ
Хмельницький національний університет
https://orcid.org/0009-0008-1049-1911
e-mail: andriydrozdit@gmail.com

МЕТОД ОРГАНІЗАЦІЇ ФУНКЦІОНУВАННЯ ОБМАННИХ СИСТЕМ З ПРИМАНКАМИ І ПАСТКАМИ В КОРПОРАТИВНИХ МЕРЕЖАХ

У роботі розроблено та обґрунтовано метод організації функціонування обманних систем із інтегрованими приманками та пастками в корпоративних мережах. Запропонований підхід спрямований на підвищення стійкості корпоративної інфраструктури до складних, у тому числі двоцільових атак, коли зловмисники поєднують розвідку та безпосередній вплив на ресурси мережі. Суть методу полягає в тому, що роботу приманок і пасток у складі обманних систем організовано динамічно, з можливістю адаптації до поведінки потенційного порушника. Для цього використано популяційні алгоритми, здатні у режимі реального часу приймати рішення щодо автоматичного блокування чи активації серверів, робочих станцій, а також відповідних пасток або приманок у момент виявлення підозрілих дій у корпоративному середовищі. Такий підхід суттєво ускладнює зловмисникам аналіз оточення, унеможливлює передбачення поведінки елементів обманної системи та підвищує шанс їхнього виведення на хибний маршрут.

Особливу увагу приділено застосуванню алгоритму «молі й полум'я» в архітектурі обманних систем як механізму вибору оптимальних подальших кроків у процесі реагування. Використання цього алгоритму дозволяє уникнути повного перебору варіантів, забезпечує швидку збіжність рішень за умов триваючих впливів, а також гарантує гнучку зміну послідовності дій залежно від актуальних змін у корпоративній мережі. Крім того, він дає змогу враховувати потенційні можливості зловмисників щодо проведення двоцільових кібератак, адаптуючи поведінку системи відповідно до рівня загрози. У результаті створюється стійкіша, інтелектуальніша та менш передбачувана архітектура оборони, здатна ефективніше протидіяти сучасним кіберзагрозам.

Перспективними напрямами подальших досліджень визначено детальне проєктування архітектури обманних систем, оптимізацію їхнього розміщення у корпоративних мережах та вдосконалення механізмів взаємодії між обманними компонентами, приманками й пастками для підвищення загального рівня кіберзахисту.

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

DROZD ANDRIY
Khmelnytskyi National University, Khmelnytskyi, Ukraine

METHOD OF ORGANIZING THE FUNCTIONING OF DECEPTIVE SYSTEMS WITH BAITS AND TRAPS IN CORPORATE NETWORKS

The work has developed and substantiated a method of organizing the functioning of deception systems with integrated baits and traps in corporate networks. The proposed approach is aimed at increasing the resistance of corporate infrastructure to complex, including dual-target attacks, when attackers combine intelligence and direct influence on network resources. The essence of the method is that the work of baits and traps as part of deception systems is organized dynamically, with the possibility of adaptation to the behavior of a potential violator. For this purpose, population algorithms were used, capable of making real-time decisions regarding the automatic blocking or activation of servers, workstations, as well as appropriate traps or baits at the moment of detection of suspicious actions in the corporate environment. This approach significantly complicates the analysis of the environment for attackers, makes it impossible to predict the behavior of the elements of the deception system, and increases the chance of leading them on the wrong route.

Special attention is paid to the application of the "moth and flame" algorithm in the architecture of deception systems as a mechanism for choosing optimal further steps in the response process. The use of this algorithm allows you to avoid a complete selection of options, ensures quick convergence of decisions under conditions of ongoing influences, and also guarantees a flexible change in the sequence of actions depending on actual changes in the corporate network. In addition, it allows you to take into account the potential opportunities of attackers to carry out dual-target cyber attacks, adapting the behavior of the system according to the level of the threat. The result is a more resilient, more intelligent and less predictable defense architecture that can more effectively counter modern cyber threats.

The detailed design of the architecture of deception systems, the optimization of their placement in corporate networks, and the improvement of mechanisms of interaction between deception components, decoys, and traps to increase the overall level of cyber protection are identified as promising directions for further research.

***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 22.10.2025
Прийнята до друку / Accepted 28.11.2025

Постановка проблеми

Перспективним та дедалі більш актуальним напрямом для забезпечення комплексної безпеки й підвищеного рівня захисту корпоративних мереж є використання спеціалізованих обманних систем, різноманітних мережних приманок і пасток для виявлення несанкціонованої активності зловмисників [1, 2]. Такі технології дають змогу не лише фіксувати атаки на ранніх етапах, а й детальніше вивчати поведінку порушників, що дозволяє краще прогнозувати їхні дії та будувати ефективніші стратегії кіберзахисту. Водночас подібні рішення є досить дороговартісними, потребують ретельного планування та передбачають ухвалення зважених управлінських рішень, оскільки їх інтеграція залежить від специфічних потреб організації, рівня її цифрової інфраструктури та вимог до забезпечення надійнішої й багаторівневої безпеки в корпоративних мережах [3, 4].

Додатковою складністю є те, що зловмисники з часом здатні адаптуватися до таких систем, виявляючи характерні ознаки пасток або моделей поведінки фальшивих вузлів мережі. Тому, для забезпечення довготривалої та ефективної експлуатації обманні системи мають бути спроєктовані таким чином, щоб вони могли функціонувати впродовж тривалого періоду, зберігати стабільність, еволюціонувати разом із середовищем та не втрачати здатність вводити зловмисників в оману. Це вимагає створення рішень, здатних самостійно приймати рішення, автоматично реагувати на зміну поведінки порушників і мінімізувати необхідність постійного втручання адміністраторів. Іншими словами, такі системи повинні володіти властивістю переходити в стан збіжності, працювати автономно та динамічно підлаштовуватися до нових загроз без залучення значних ресурсів [5, 6].

Аналіз останніх досліджень і публікацій

У роботі [7] кібербезпека визначена як нова проблема для управління інформаційними технологіями в бізнесі та суспільстві завдяки швидкому розвитку телекомунікаційних та бездротових технологій. Безпека кіберпростору мала вплив на численні ключові інфраструктури. Поряд із даними про поточний стан безпеки, система повинна отримувати історичні дані для впровадження новітнього захисту та захисту в галузі кібербезпеки. Вона також приймає інтелектуальні рішення, які можуть забезпечити адаптивне управління безпекою та контроль. У роботі розроблено інтелектуальну систему кібербезпеки з використанням налаштування гіперпараметрів на основі методу регуляризованої довгої короткострокової пам'яті для підвищення рівня безпеки основних системних активів. Для підвищення ефективності прийняття рішень щодо виявлення атак було вирішено проблему суперечливих або неструктурованих даних.

Кіберстійкість [8] у хмарних обчисленнях є однією з найважливіших можливостей корпоративної мережі, яка забезпечує постійну здатність протистояти несприятливим умовам та швидко відновлюватися після них. Цю здатність можна виміряти за допомогою методів оцінки ризиків кібербезпеки. Однак дослідження управління ризиками кібербезпеки в підходах до стійкості хмарних обчислень є недостатніми. Запропонована робота намагається виявити вразливості хмари, оцінити загрози та виявити компоненти високого ризику, щоб нарешті запропонувати відповідні заходи безпеки, такі як прогнозування та усунення збоїв, методи резервування або балансування навантаження для швидкого відновлення та повернення до стану, що був до атаки, якщо станеться збій.

У роботі [9] розглянуто клас мереж, які можуть бути створені в паралельному часі за допомогою конструкторів мереж. Починаючи з порожньої мережі, метою роботи була побудова стабільної мережі, яка належить до заданої підмножини. У роботі [10] проаналізовано чотири парадигми паралельних обчислень – гетерогенні обчислення, квантові обчислення, нейроморфні обчислення та оптичні обчислення. Було розглянуто нові розподілені системи, такі як блокчейн, безсерверні обчислення та хмарні архітектури. У роботі [11] представлено дослідження комплексного, динамічного та багаторівневого підходу до оцінки та моделювання кіберризиків у розподілених інформаційних системах на основі метрик безпеки та методів їх розрахунку, який забезпечує достатню точність та надійність оцінки ризиків і демонструє здатність вирішувати задачі інтелектуальної класифікації та моделювання оцінки ризиків для великих масивів розподілених даних.

У роботі [12] розглянуто проблеми інтелектуальних мереж щодо кіберфізичних систем та систем кібербезпеки, стандартних протоколів, комунікаційних та сенсорних технологій. Існуючі методи машинного навчання на основі навчання з учителем для виявлення кібератак в інтелектуальних мережах здебільшого спираються на випадки як нормальних, так і атакуючих подій для навчання. Крім того, щоб навчання з учителем було ефективним, навчальний набір даних повинен містити репрезентативні приклади різних ситуацій атаки з різними закономірностями, що є складним завданням. Тому, в роботі запропоновано новий підхід до інтелектуального аналізу даних, який заснований на правилах без учителя для виявлення кібератак з введенням помилкових даних в інтелектуальних мережах.

У роботі [13] досліджуються фундаментальні вимоги до зв'язку, структури та протоколи, необхідні для встановлення безпечного з'єднання в мікромережах. Крім того, оцінюється інтеграція різноманітних методів безпеки. У статті представлено тематичне дослідження, яке ілюструє впровадження розподіленої системи кібербезпеки в умовах мікромережі. У роботі [14] розглянуто проблеми мережного ризику, з якими стикаються кіберсистеми, Враховуючи можливі вразливості кібератак пропонується динамічний байєсівський мережний підхід для кількісної оцінки ризику безпеки КФС розподільчої мережі. У роботі [15] розглянуто нові обчислювальні парадигми, такі як безсерверні обчислення, периферійні обчислення та обчислення на основі блокчейну. У роботі [16] представлено інноваційну стратегію захисту для активних розподільчих мереж, що використовує принципи розподіленої координації та багатоагентних систем. Запропонована стратегія складається з двох етапів. Перший етап включає алгоритм виявлення несправностей, який спирається виключно на локальні вимірювання, тоді як другий етап використовує класифікацію агентів для обчислення оптимального часу роботи на основі динамічного матричного представлення шляху несправності в поєднанні зі спрощеною задачею розподіленої оптимізації. Процес координації сформульовано як набір задач лінійної оптимізації, що спрощує рішення. У роботі [17] розглянуто розподілений закон керування на основі адаптивного керування на основі моделі для керування набором агентів з динамікою подвійного інтегратора за схемою "лідер-слідуваний" за наявності системних аномалій, таких як невизначеності, пов'язані з агентами, невідома ефективність керування та динаміка виконавчих механізмів. Показано стійкість загальної замкнутої багатоагентної системи, використовуючи теорію стійкості Ляпунова.

Сфера [18] самоадаптивного програмного забезпечення стає дедалі важливішою, оскільки програмне забезпечення повинно адаптувати свою поведінку під час виконання, щоб встигати за динамічними та постійно мінливими середовищами. Здатність програмного забезпечення до самомодифікації та налаштування відома як адаптивність, що визнано важливим атрибутом якості. Ступінь, до якої архітектура може адаптуватися до змін, буде ключовим фактором у визначенні адаптивності програмного забезпечення. В роботі запропоновано комплексний підхід до оцінки адаптивності архітектури програмного забезпечення.

У роботі [19] розглянуто проблеми безпеки, такі як несанкціонований доступ, а також проблеми конфіденційності, які створюють значні перешкоди. Їх можна подолати, впроваджуючи методи контролю доступу та динамічну політику безпеки та конфіденційності, яка регулює ці проблеми там, де вони виникають. У цій роботі запропоновано алгоритм навчання з учителем на основі прийняття рішень щодо політик та контролю доступу. Безпека контролю доступу покращується завдяки тому, що він стає динамічним, адаптивним, гнучким та розподіленим. У роботі [20] розглянуто самоорганізацію у складних системах. Це процес, який пов'язаний зі зниженням внутрішньої ентропії та виникненням структур, які можуть дозволити системі функціонувати ефективніше та стійкіше у своєму середовищі та більш конкурентно з іншими станами системи або з іншими системами.

Метою роботи є підвищення ефективності функціонування обманних систем з приманок та пасток в корпоративних мережах для виявлення ЗПЗ та КА.

Виклад основного матеріалу

Організація систем виявлення комп'ютерних атак та зловмисного програмного забезпечення в корпоративних мережах потребує удосконалення на рівні архітектури, особливо при використанні приманок і пасток для покращення протидії зловмисникам. Корпоративні мережі з великою кількістю вузлів та посиленим захистом за рахунок підтримки великої кількості приманок та пасток потребують швидкого та ефективного управління ними.

Приманки можуть використовуватись не тільки для відволікання зловмисників та неправильного розуміння ними хибних об'єктів, але й для того, щоб при проведенні зловмисниками атак перенаправити або продублювати трафік на приманки, які є невидимими зловмисникам, з подальшим аналізом трафіку та прийняття відповідних дій. Також, при цьому можуть бути активізовані пастки в поєднанні з приманками. Приманки можуть бути різними та мати різну будову, тому система повинна оцінити їх та здійснити вибір найбільш ефективних з них. Для здійснення вибору приманок з пастками можуть бути застосовані різні стратегії. Але в цьому процесі важливим є вибір саме таких варіантів приманок з пастками, які б могли в процесі проведення атак, привести не тільки до однієї певної приманки. Взагалі приманки з пастками можуть бути досліджені зловмисниками і дуже багато з них не мають повноцінних наборів правильних відповідей, які повинні імітувати, і тому, вони можуть бути зрозумілими зловмисникам через їх виявлення, а в частих випадках і використані ними для зловмисних дій. Тому, керування приманками з пастками має бути організовано з врахуванням спроможності досліджувати комп'ютерні атаки сукупністю таких об'єктів за певними стратегіями. Перспективним напрямом для дослідження таких стратегій є стратегії, що базуються на використанні популяційних алгоритмів в архітектурі систем виявлення комп'ютерних атак з приманками і пастками.

Розглянемо побудову моделі комп'ютерних двоцільових атак в корпоративних мережах з системами приманок і пасток. Зловмисники в процесі організації та проведення атак на корпоративні мережі спрямовуються на використання вразливостей систем, викрадення конфіденційної інформації і порушення штатного функціонування корпоративних інформаційних та комп'ютерних систем і мереж. Для організації атак застосовують типові інструменти з використанням автоматизованих сценаріїв та засобів для здійснення атак на велику кількість об'єктів в глобальній мережі або зловмисник використовує клавіатуру для цілеспрямованої початкової спроби доступу і виконання подальших дій. Розглядатимемо мережні атаки винятково на корпоративні мережі і з врахуванням того, що вони можуть бути пасивними і активними, тобто КА, а також з використанням ЗПЗ і спрямованими на перехоплення трафіку. До пасивних атак віднесемо сканування портів, а до активних атак - DDoS-атаки і атаки на основі паролів. Тому, будемо розглядати КА як мережні атаки і атаки з використанням ЗПЗ.

В корпоративних мережах можуть бути розміщені різні системи та засоби протидії комп'ютерним атакам і зловмисним діям. Корпоративні мережі можуть мати різні стани захищеності ресурсів та вузлів. Розглядатимемо ті з них, які мають високий рівень захищеності, для забезпечення якого в мережах обов'язково встановлені системи з приманками і пастками. Така організація захисту не є типовою та поширеною, але стає все більш актуальною із зростанням та появою нових типів комп'ютерних атак і зловмисних загроз. Застосування окремих приманок і пасток або систем з приманками і пастками вимагає додаткових витрат від власників корпоративних мереж, але такі витрати покращують рівень захисту і безпеку в корпоративних мережах порівняно з корпоративними мережами без них. Для досягнення ефекту з протидії комп'ютерним атакам загальноприйнято встановлювати не менше п'ятнадцяти відсотків приманок від загальної кількості вузлів в комп'ютерних мережах. Така кількість приманок потребує системи з керування їх застосуванням. Самі приманки і пастки можуть бути однаковими, але можуть бути і повністю різними за будовою, призначенням, місцем встановлення, способами та етапами застосування тощо. Приманки можуть містити пастки або застосовуватись разом з пастками чи без них. Складними завданнями із застосування приманок і пасток є спрямування зловмисника на них. Не завжди приманки можуть бути активізовані під час здійснення комп'ютерних атак. Все це необхідно враховувати в архітектурі систем з приманками і пастками для забезпечення їх застосування.

Приманки мають різну будову в залежності від призначення і застосування. Їх можна поділяти на дві групи: низького рівня взаємодії; високого рівня взаємодії. Або на три такі групи в залежності від рівнів взаємодії: низького; середнього; високого. Приманки з низьким рівнем взаємодії мають обмежену симуляцію обслуговування та невеликі експлуатаційні витрати. Приманки з середнім рівнем взаємодії забезпечують розширене моделювання, збір цільового профілю пристрою. До приманок з середнім рівнем взаємодії відносять ті з них, які забезпечують функції послуг від тих, які надають приманки з високим рівнем, до послуг, які надають приманки з низьким рівнем взаємодії. Приманки з високим рівнем взаємодії забезпечують майже повноцінні послуги і, тому, виступають цілями в корпоративних мережах. Всі приманки забезпечують моделювання послуг або певних систем за рахунок закладеного в них механізму обману. Але до якого б рівня вони не відносились і скільки їх не було б в корпоративних мережах, зловмисники при проведенні атак можуть встановити несправжність цих об'єктів в корпоративних мережах, а також використати це в своїх цілях зі зворотньою до їх призначення метою.

Для дослідження корпоративних мереж та їх ресурсів зловмисники можуть використовувати доступні стандартні засоби і на їх основі, відповідно, реалізовувати активні чи пасивні методи дослідження або їх поєднання. При реалізації активних методів використовують набори команд і засобів, які взаємодіють із системою, для виклику конкретних реакцій, щоб сформувати характеристику системи. При застосуванні пасивних методів дані про систему отримують з мережного трафіку або метадані із зовнішніх баз даних тощо. Таким чином, для вивчення корпоративних мереж зловмисники можуть використовувати різні методи окремо або поєднувати їх. Якщо корпоративні мережі містять системи з приманками та пастками або окремі приманки з пастками, то зловмисники теж можуть досліджувати їх наявність під час здійснення початкових етапів атак. Реалізація приманок як повноцінних об'єктів є складним завданням і, тому, для його спрощення розробники частину функцій або елементів повноцінних об'єктів не реалізовують. Часто реалізовані функції чи елементи приманок можуть бути примітивними. Тому, зловмисники в процесі дослідження корпоративних мереж або при проведенні активної фази атак досліджують та встановлюють компоненти систем з приманками та пастками. Це понижує ефективність такого підходу до протидії КА та зловмисним проявам і потребує вдосконалення архітектури систем з приманками та пастками для забезпечення їх ефективної організації, враховуючи обмежені спроможності окремих приманок та пасток.

Для КА загально прийнято, що вони реалізуються переважно в три етапи: розвідка; атака; завершення атаки. Кожен етап КА є важливим. На етапі розвідки зловмисники обов'язково досліджують системи і засоби захисту корпоративних мереж, зокрема і оточення визначених для атак об'єктів. Об'єктами комп'ютерних атак є комп'ютерні системи загалом та їхні компоненти, інформаційні ресурси, дані, програмне та технічне забезпечення, а також комп'ютерні пристрої та мережі. Метою атак зловмисників на корпоративні мережі можуть бути спроби порушити конфіденційність інформації для отримання несанкціонованого доступу до неї, порушити цілісність інформації для її зміни чи знищення, а також порушити доступність інформації, здійснюючи несанкціоноване блокування доступу до системи або даних. Всі ці цілі зловмисників є актуальними і можливими для реалізації в контексті корпоративних мереж з різними ступенями захисту.

Задамо модель комп'ютерних атак з урахуванням цілей зловмисників, що стосуються порушення конфіденційності, цілісності та доступності інформації в корпоративних мережах, так:

$$M_{KA,1} = \langle R_{kn}, R_p, G_{kn,p}, K_{a,1}, G_{ka,1} \rangle, \quad (1)$$

де R_{kn} – множина об'єктів корпоративних мереж, які можуть піддані комп'ютерним атакам; R_p – множина хибних об'єктів для комп'ютерних атак, тобто приманок і приманок з пастками; $G_{kn,p}$ – граф зв'язків між об'єктами корпоративних мереж та хибними об'єктами для комп'ютерних атак; $K_{a,1}$ – множина векторів комп'ютерних атак на об'єкти корпоративних мереж; $G_{ka,1}$ – граф зв'язків джерел комп'ютерних атак зловмисників та потенційних об'єктів корпоративних мереж з урахуванням векторів комп'ютерних атак.

Комп'ютерні атаки, які задано моделлю $M_{KA,1}$ за формулою (1), віднесемо до одноцільових атак за умови, що вони спрямовані винятково на реальні об'єкти корпоративних мереж і не спрямовані на хибні об'єкти. Таким чином, якщо зловмисники спрямовуватимуть свої атаки тільки на реальні об'єкти корпоративних мереж, серед яких можуть бути і хибні об'єкти, то такі комп'ютерні атаки вважатимемо одноцільовими.

В контексті використання в корпоративних мережах систем з приманками і пастками КА можуть бути спрямовані не тільки на визначені об'єкти, але й на приманки та пастки з метою їх використання в процесі продовження виконання КА. Для цього на етапі розвідки такі об'єкти можуть бути виявлені і за результатами виявлення скориговані цілі та моделі КА. Таким чином, КА може мати дві цілі: запланований об'єкт для атаки; додатковий (хибний) об'єкт для атаки (приманки). Такі КА будемо називати двоцільовими і введемо їх загальну модель так:

$$M_{KA,2} = \langle R_{kn}, R_p, G_{kn,p}, K_{a,2}, G_{ka,2} \rangle, \quad (2)$$

де R_{kn} – множина об'єктів корпоративних мереж, які можуть піддані комп'ютерним атакам; R_p – множина хибних об'єктів для комп'ютерних атак, тобто приманок і приманок з пастками; $G_{kn,p}$ – граф зв'язків між об'єктами корпоративних мереж та хибними об'єктами для комп'ютерних атак; $K_{a,2}$ – множина векторів комп'ютерних атак на об'єкти корпоративних мереж та хибні об'єкти для комп'ютерних атак; $G_{ka,2}$ – граф зв'язків джерел комп'ютерних атак зловмисників, потенційних та хибних об'єктів корпоративних мереж з урахуванням векторів комп'ютерних атак.

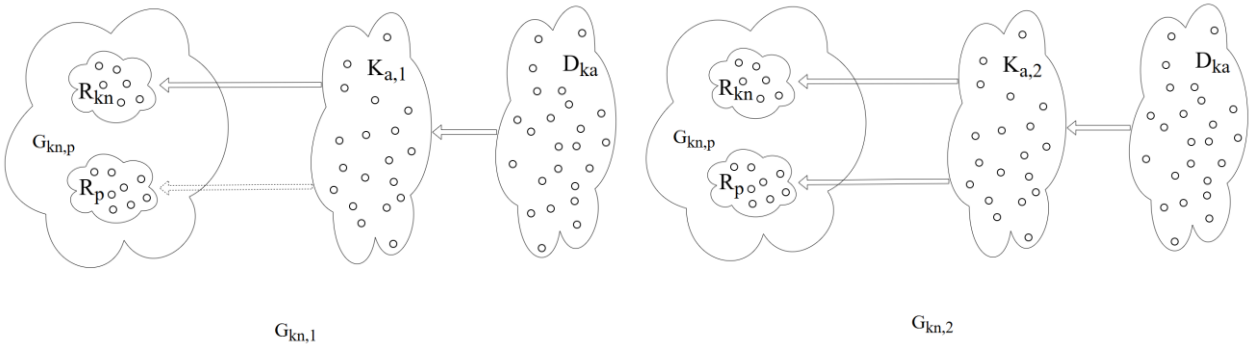
В формулі (1) множина R_p може бути порожньою або не порожньою. А в формулі (2) ця множина R_p завжди є непорожньою. Множини R_{kn} та R_p в формулах (1) та (2) є однаковими. Граф зв'язків $G_{kn,p}$ між об'єктами корпоративних мереж та хибними об'єктами для комп'ютерних атак в формулах (1) та (2) є однаковим і відображає зв'язки між в корпоративних мережах в контексті взаємодії для забезпечення захисту і безпеки.

В формулі (1) граф зв'язків $G_{ka,1}$ джерел комп'ютерних атак зловмисників та потенційних об'єктів корпоративних мереж з урахуванням множини векторів $K_{a,1}$ комп'ютерних атак на об'єкти корпоративних мереж не враховує спрямування зловмисників на пошук хибних об'єктів атак, тобто приманок і пасток. В формулі (2) граф зв'язків $G_{ka,2}$ джерел комп'ютерних атак зловмисників, потенційних та хибних об'єктів корпоративних мереж з урахуванням множини векторів $K_{a,2}$ комп'ютерних атак на об'єкти корпоративних мереж враховує спрямування зловмисників на пошук хибних об'єктів атак, тобто приманок і пасток, з метою їх подальшого використання. Таким чином, в другому випадку модель КА враховує дві цілі. Таку потенційну поведінку зловмисників повинні враховувати при проєктуванні захисту корпоративних мереж із використанням приманок і пасток як хибних об'єктів для КА.

Логіка дій зловмисника в першому випадку, який задано за формулою (1), полягає в тому, що зловмисник в процесі здійснення атаки не здійснює пошук хибних об'єктів для атак в корпоративних мережах. Він спрямований безпосередньо на досягнення мети і тому він в процесі здійснення атаки може не досягти мети через технічну неспроможність або попавши на хибні об'єкти для атак. Якщо він попадає на хибні об'єкти для атак, то в даному випадку він може знати або не знати про такий розвиток подій. Але при цьому він не розглядав їх наявність як засобів для досягнення мети. В другому випадку зловмисник в своїй моделі атаки закладає можливість поділу об'єктів корпоративних мереж на основні об'єкти та хибні об'єкти для атак. Модель такої атаки зі сторони зловмисника має на меті розроблення додаткового етапу атаки, що полягає в класифікації об'єктів в корпоративних мережах для покращення результативності при здійсненні атаки. Подальші дії зловмисника будуть зосереджені на використанні знайдених ним хибних об'єктів для атак в корпоративних мережах для удосконалення планованої атаки, що потребуватиме від нього розроблення додаткового етапу КА. Таким чином, зловмисник після здійснення власної класифікації об'єктів в корпоративних мережах на два класи повинен здійснювати окремі дії з дослідження хибних об'єктів для атак. З іншої сторони, тобто зі сторони хибних об'єктів для атак, особливо якщо вони інтелектуальні, можуть бути дії, які будуть спонукати зловмисника до витрат ресурсів і часу. Крім того, зловмиснику буде складно провести чітку класифікацію реальних та хибних об'єктів в корпоративних мережах. Це теж повинно бути враховано в моделі захисту корпоративних мереж, а також в моделі зловмисних дій.

Відмінність між обома моделями поведінки зловмисника є суттєвою. Але при цьому складно відокремити особливість, яка характеризує другий випадок. Тому, в першому випадку можна здійснити припущення, що зловмисник цілеспрямований винятково щодо результатів атаки і не поділяє об'єкти корпоративних мереж, бо це може бути не пов'язано з його кваліфікацією, а саме винятково із метою атаки. Вважатимемо, що кваліфікація зловмисника в обох випадках є однаковою. Тоді, наприклад, метою атаки в першому випадку можуть бути відповідно до властивостей інформації такі загрози: цілісності, що пов'язані із знищенням або модифікацією інформації; загрози доступності, які пов'язані із блокуванням чи знищенням. А в другому випадку до цих загроз для інформації можна додати ще загрози для конфіденційності, які полягають в спробах здійснити несанкціонований доступ, витік або розголошення. Ці загрози для інформації вибілено в другому випадку, бо для їх успішного забезпечення зловмиснику потрібно буде після проведення атаки продовжувати здійснення комунікації з об'єктами корпоративних мереж, тому порівняно з першим випадком обсяг робіт, витрати часу та ресурсів будуть більшими. Крім того, розглядувані загрози для інформації в другому випадку будуть включати всі загрози і першого випадку. В першому випадку теж можуть бути метою КА реалізовані загрози для конфіденційності, але оскільки вони спрямовані на несанкціонований доступ, витік або розголошення, то через наявність хибних об'єктів атак та довшу тривалість для забезпечення досягнення мети щодо порушення конфіденційності вони можуть мати суттєво менший успіх. Таким чином, для забезпечення безпеки та захисту корпоративних мереж з використанням хибних об'єктів атак потрібно враховувати, що модель КА переважно буде двоцільовою.

Графи зв'язків $G_{ka,1}$ та $G_{ka,2}$ зобразимо на рис. 1 у відповідності до моделей (формули (1) і (2)).



а) одна ціль б) дві цілі

Рис.1. Графічне подання компонентів моделей $M_{KA,1}$ та $M_{KA,2}$

На рис. 1 для КА виділено окремо множину джерел атак D_{KA}, з елементів якої зловмисники проводять свої атаки, задані елементами в множинах $K_{a,1}$ та $K_{a,2}$. Джерел КА може бути декілька, а може бути одне. В контексті моделей $M_{KA,1}$ та $M_{KA,2}$ це не є принциповим, оскільки важливим є тільки наявність мети у зловмисників та відповідних засобів для пошуку і здійснення КА безпосередньо на хибні об'єкти для атак в корпоративних мережах. Отже, відношення джерел КА до об'єктів корпоративних мереж можуть бути «один до одного», «один до всіх», «всі до одного» та «всі до всіх», якщо розглядати елементи множин R_{kn} та R_p як окремі різні об'єкти. Таких об'єктів є небагато в контексті саме різних, тоді варіантів відношень джерел КА до них теж буде небагато. Варіантів доступу до об'єктів може бути багато, а самих об'єктів, які цікавлять зловмисників в корпоративних мережах небагато. Таким чином, при здійснені КА на корпоративні мережі з метою пошуку та взяття під контроль або для нейтралізації хибних об'єктів для КА формується нова друга ціль, реалізація якої відрізняється віл цілі щодо основних об'єктів для КА тим, що може бути здійснена типовими підходами для елементів множини R_p.

Деталізуємо множини в формулах (1) та (2) їх елементами для задання відповідності саме між елементами. Нехай $R_{kn} = \{r_{kn,1}, r_{kn,2}, \dots, r_{N_{R_{kn}}}\}$, де $N_{R_{kn}}$ – кількість об'єктів корпоративних мереж, на які можуть бути спрямовані КА зловмисників, та $R_p = \{r_{p,1}, r_{p,2}, \dots, r_{N_{R_p}}\}$, де N_{R_p} – кількість хибних об'єктів для КА в корпоративних мережах. Граф зв'язків $G_{kn,p}$ між об'єктами корпоративних мереж та хибними об'єктами для комп'ютерних атак задамо так:

$$G_{kn,p} = \{(a,b) | \; if \; f_{G_{kn,p}}(a,b) = 1, a \neq b, \forall a \in R_{kn} \cup R_p, \forall b \in R_{kn} \cup R_p, R_{kn} \cap R_p = \emptyset\}, \quad (3)$$

де $f_{G_{kn,p}}(a,b)$ – бітова функція, що відображає зв'язок між елементами $a \in R_{kn} \cup R_p$ та $b \in R_{kn} \cup R_p$, і її значення визначаються так, що при наявності зв'язку між елементами $f_{G_{kn,p}}(a,b) = 1$, а при відсутності $f_{G_{kn,p}}(a,b) = 0$.

За формулою (3) встановлюється топологія між об'єктами в корпоративних мережах, які можуть бути піддані КА, включно з хибними об'єктами для КА. Частина елементів множин R_{kn} та R_p можуть розміщені в одних і тих же комп'ютерних станціях в корпоративних мережах. Але елементи множин R_{kn} та R_p не можуть належати обом множинам одночасно, тобто $R_{kn} \cap R_p = \emptyset$. Елементи a, b не можуть бути однаковими в формулі (3), бо тоді такий випадок відповідатиме ізольованій вершині з петлею в графі $G_{kn,p}$ і, відповідно, для такого елементу зв'язку з рештою об'єктів не буде, включно з підсистемою організації та взаємодії між елементами, що неможливо згідно визначення елементів множин R_{kn} та R_p. Множини R_{kn} та R_p формують два класи об'єктів.

Визначимо елементами множину векторів $K_{a,1}$ комп'ютерних атак на об'єкти корпоративних мереж так: $K_{a,1} = \{k_{a,1,1}, k_{a,1,2}, \dots, k_{a,1,N_{K_{a,1}}}\}$, де $N_{K_{a,1}}$ – кількість векторів КА, які можуть здійснити зловмисники. Також, визначимо елементами множину векторів $K_{a,2}$ комп'ютерних атак на об'єкти корпоративних мереж та хибні об'єкти для комп'ютерних атак так: $K_{a,2} = \{k_{a,2,1}, k_{a,2,2}, \dots, k_{a,2,N_{K_{a,2}}}\}$, де $N_{K_{a,2}}$ – кількість векторів КА, які можуть здійснити зловмисники. Згідно цих визначень та формул (1) і (2) множина $K_{a,2}$ буде включати множину $K_{a,1}$, тобто множина $K_{a,1}$ є підмножиною множини $K_{a,2}$. Тоді, частина векторів КА з множини $K_{a,2}$ буде стосуватись винятково хибних об'єктів для КА в корпоративних мережах.

Граф зв'язків $G_{ka,1}$ джерел комп'ютерних атак зловмисників та потенційних об'єктів корпоративних мереж з урахуванням множини $K_{a,1}$ векторів комп'ютерних атак у формулі (1) задамо так:

$$G_{ka,1} = \{(a,b) | \; if \; f_{G_{ka,1}}(a,b) = 1, a \neq b, \forall a \in K_{a,1}, \forall b \in R_{kn}, K_{a,1} \cap R_{kn} = \emptyset\}, \quad (4)$$

де $f_{G_{ka,1}}(a,b)$ – бітова функція, що відображає зв'язок між елементами $a \in K_{a,1}$ та $b \in R_{kn}$, і її значення визначаються так, що при наявності зв'язку між елементами $f_{G_{ka,1}}(a,b) = 1$, а при відсутності $f_{G_{ka,1}}(a,b) = 0$.

Граф зв'язків $G_{ka,2}$ джерел комп'ютерних атак зловмисників, потенційних та хибних об'єктів корпоративних мереж з урахуванням векторів комп'ютерних атак згідно множини $K_{a,2}$ векторів КА у формулі (2) задамо так:

$$G_{ka,2} = \{(a,b) | \; if \; f_{G_{ka,2}}(a,b) = 1, a \neq b, \forall a \in K_{a,2}, \forall b \in R_{kn} \cup R_p, R_{kn} \cap R_p = \emptyset, K_{a,2} \cap R_p = \emptyset, K_{a,2} \cap R_{kn} = \emptyset\}, \quad (5)$$

де $f_{G_{ka,2}}(a,b)$ – бітова функція, що відображає зв'язок між елементами $a \in K_{a,2}$ та $b \in R_{kn} \cup R_p$, і її значення визначаються так, що при наявності зв'язку між елементами $f_{G_{ka,2}}(a,b) = 1$, а при відсутності $f_{G_{ka,2}}(a,b) = 0$.

КА згідно заданого графу $G_{ka,2}$ в формулі (5) порівняно із заданням графу $G_{ka,1}$ в формулі (4) можуть бути здійснені безпосередньо на елементи множини R_{kn}, на елементи множини R_p та на елементи множини R_{kn} через елементи множини R_p або з їх залученням. Наприклад, на рис. 2 зображено ці три варіанти за умови вирішення завдань атаки від джерела до об'єктів. На рис. 3 зображено ці ж варіанти за умови встановлення взаємодії джерела атаки з об'єктами корпоративних мереж. Якщо ж розглядати граф $G_{ka,1}$, то можливий лише один варіант здійснення КА, тобто безпосередньо на елементи множини R_{kn}. Якщо серед об'єктів при здійсненні КА в цьому випадку з графом $G_{ka,1}$ будуть траплятись хибні об'єкти з множини R_p, то зловмисниками вони можуть прийняті як важливі об'єкти в корпоративних мережах або будуть відхилені. Якщо вони будуть прийняті як важливі об'єкти, то протягом певного часу КА активує приманки чи пастки, що

забезпечить для зловмисників втрату часу та планованого результату КА. В цьому випадку зловмисник не використовує засоби проведення КА безпосередньо на хибні об'єкти для КА в корпоративних мережах.

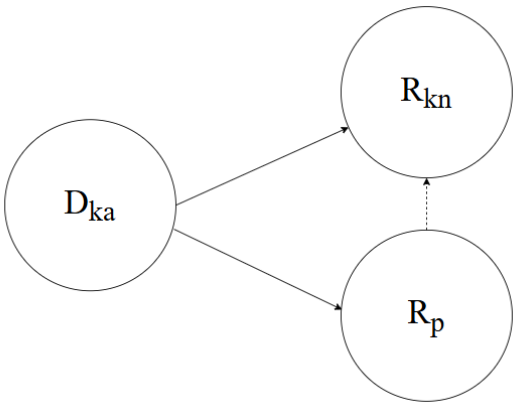


Рисунок 2 – Граф трьох варіантів КА згідно формули (5) на основі односторонніх зв'язків

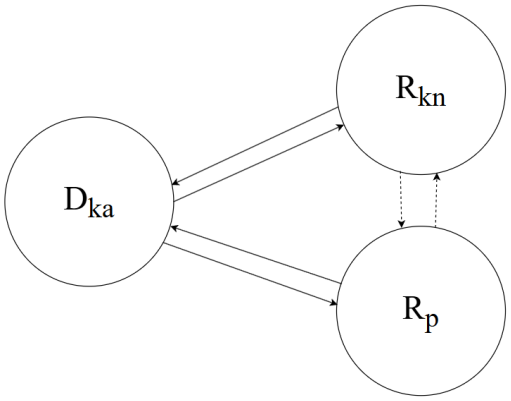


Рисунок 3 – Граф трьох варіантів КА згідно формули (5) на основі багатосторонніх зв'язків

Елементи множин R_{kn}, R_p, D_{KA} після встановлення відповідних з'єднань, тобто деталізації КА, задамо матрицями інцидентності. В результаті отримаємо базу поведінкових сигнатур КА. Згідно формули (2) визначимо місце двоцільових КА серед типових етапів КА.

1. Етап розвідки, на якому зловмисник здійснює збір даних з відкритих джерел, шляхом зондування комп'ютерних мереж або перехопленням мережного трафіку для аналізу.

2. Етап класифікації об'єктів корпоративних мереж з метою виділення реальних та хибних об'єктів корпоративних мереж.

3. Етап доставлення спеціалізованого ЗПЗ із застосуванням різних способів та засобів на реальні та хибні об'єкти корпоративних мереж.

4. Етап приховування КА та доставлення спеціалізованого ЗПЗ.

5. Етап використання виявлених вразливостей в системі корпоративних мереж, зокрема і хибних об'єктів для атак.

6. Етап встановлення спеціалізованого ЗПЗ на реальні та/або хибні об'єкти корпоративних мереж.

7. Етап встановлення зв'язку між джерелом атаки та об'єктами корпоративних мереж.

8. Етап використання зловмисником контрольованих хибних об'єктів корпоративних мереж для розвідки реальних об'єктів.

9. Проведення внутрішньої розвідки в корпоративних мережах.

10. Етап обходу внутрішнього захисту комп'ютерних станцій корпоративних мереж.

11. Етап використання виявлених вразливостей комп'ютерних станцій корпоративних мереж.

12. Етап підвищення привілеїв.

13. Етап доступу до облікових даних.

14. Етап проведення розвідки згідно отриманих внутрішніх даних.

15. Етап обходу внутрішнього захисту на досягнутому об'єкті корпоративних мереж.

16. Етап використання виявлених вразливостей на досягнутому об'єкті корпоративних мереж.

17. Етап здійснення впливу на об'єкті, зокрема хибному об'єкті, корпоративних мереж, що включає також отримання та фіксування контролю над ним.

18. Етап завершення КА, який може мати варіант повного завершення або завершення в контексті утримання комп'ютерних станцій корпоративних мереж під контролем.

Таким чином, поділ зловмисниками на реальні та хибні об'єктів корпоративних мереж збільшує кількість етапів проведення КА, але при цьому дає їм можливість ефективніше їх здійснювати, залучаючи також для атак наявні хибні об'єкти над якими вони отримали контроль.

У випадку неправильної класифікації об'єкту, що відноситься до хибних об'єктів для атак, і за наявності в нього високого ступеня інтеграції зловмисник може отримати проблеми з проведенням КА. Такий хибний об'єкт може містити різні шарі обману, зокрема такі, що імітують мережу, чи систему, чи програмне забезпечення, чи дані. При цьому такий хибний об'єкт може комунікувати зі зловмисником, вводячи його в оману та в результаті спонукає витрачати час та ресурси. Така модель взаємодії повинна бути врахована зловмисником і розробниками/адміністраторами систем безпеки та захисту корпоративних мереж. Наприклад, для зловмисників це можуть бути етапи 3, 7, 8, на яких зловмисник вважає, що він контролює хибний об'єкт для атак чи реальний об'єкт, а реально об'єкт надає йому певний шар обману.

Тому, розроблена модель двоцільових КА включає особливості в захисті корпоративних мереж, які пов'язані із використанням хибних об'єктів для атак та їх включенням в сценарій КА з виділенням певних етапів. Це дає змогу зловмиснику не тільки здійснювати поділ на реальні та хибні об'єкти в корпоративних мережах, але й згідно розроблюваного сценарію КА залучати хибні об'єкти, які взяті під його контроль, для виконання своїх подальших дій. Такі дії зловмисника повинні бути враховані розробниками систем безпеки та

захисту корпоративних мереж, в яких використовуються додатково хибні об'єкти для атак. Організація керування і взаємодії таких хибних об'єктів для атак та їх внутрішня архітектура повинні враховувати дії зловмисника, які базуються на розробленій загальній моделі двоцільових КА, що потребує розроблення нової архітектури системи керування та взаємодії хибних об'єктів для атак в корпоративних мережах з врахуванням її таких особливостей.

Розглянемо метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах для виявлення двоцільових атак. Функціонування обманних систем з приманками і пастками в корпоративних мережах потребує забезпечення взаємодії їх розподілених компонентів, підтримування тривалого часу функціонування в змінюваному середовищі, опрацюванні штатних і позаштатних подій в оточуючому середовищі та при взаємодії між компонентами систем, виконання визначених функцій з виявлення КА та ЗПЗ, реалізації обманних дій та керування приманками і пастками. В поєднанні ці основні функції обманних систем повинні забезпечити організацію функціонування обманних систем з приманками і пастками протягом тривалого часу та в умовах впливів КА та дій ЗПЗ.

Комп'ютерні станції в корпоративних мережах можуть бути увімкнені в різний час, а сервери можуть працювати цілодобово. Якщо виокремити приманки і пастки, то вони можуть бути активними в увімкнених комп'ютерних станціях, які цілеспрямовано не вимикаються для їх підтримки в цілодобовому режимі. Також вони можуть вимикатись разом з рештою комп'ютерних станцій. Тому, виникає проблема щодо можливості класифікації реальних та хибних об'єктів в корпоративних мережах через різні добові графіки увімкнень серверів, комп'ютерних станцій тощо, а також через атаки, які здійснюються з різних часових поясів. Для уникнення таких дій, обманні системи повинні функціонувати в корпоративних мережах цілодобово із залученням додаткових ресурсів, зокрема додатково до необхідних функціонуючих серверів повинні бути долучені комп'ютерні станції з елементами та компонентами обманних систем з приманками і пастками. А також, приймати рішення 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. Обманні системи повинні підтримувати імітацію функціонування корпоративних мереж у неробочий для користувачів час. Таким чином, застосування обманних систем з приманками і пастками повинно здійснювати цілодобово. Долучення нових комп'ютерних станцій або вилучення наявних в корпоративні мережі може бути здійснено без вимкнення всіх вузлів. Долучення нових комп'ютерних станцій в корпоративні мережі повинно супроводжуватись встановлення компонентів та елементів обманних систем, включно з встановленням приманок і пасток за потреби. При вилученні комп'ютерних станцій чи серверів з корпоративних мереж повинні бути скориговані відомості про вузли та їх типи в базах обманних систем. Всі такі дії впливають на оцінювання рівнів безпеки вузлів та всієї мережі в цілому. При зміні вузлів в корпоративних мережах та, відповідно, і архітектури обманних систем з приманками і пастками системи оновлюють відомості про стани та параметри оточуючого середовища та внутрішні процеси. Також, для підтримуванні цілісності розподілених компонентів обманних систем в них здійснюються постійні обміни повідомленнями щодо поточних станів і подій, які стосуються винятково їх.

Обманні системи повинні здійснювати опрацювання штатних і позаштатних подій в оточуючому середовищі та при взаємодії між компонентами систем, які стосуються їх функціонування, без залучення адміністраторів. Якщо ж все-таки залучення адміністраторів необхідне, тоді обманні системи повинні локалізувати вузли корпоративних мереж і надати повідомлення адміністраторам. Якщо ж обманні системи зіткнулись з внутрішніми проблемами свого функціонування і не змогли вирішити їх, тобто не змогли опрацювати позаштатні події, тоді теж залучають адміністраторів, блокуючи при цьому більшість або всі вузли, в які вони встановлені їх компоненти та елементи.

Для виконання визначених функцій з виявлення КА та ЗПЗ обманні системи повинні мати набір ознак для розпізнавання впливів КА чи дій ЗПЗ. Кількість функцій для опрацювання таких подій не є обмеженою і в систему можна їх доповнювати. Нові функції можуть бути доповнені через долучення нових елементів чи компонентів в комп'ютерні станції або з долученням нових комп'ютерних станцій. Окремі функції можуть бути розподілені між компонентами обманних систем або бути включеними до складу приманок і пасток.

Обманні системи з приманками і пастками окремо від приманок і пасток повинні мати набір обманних дій, які вони повинні застосовувати для заплутування зловмисників при проведенні КА чи дій ЗПЗ. Також, в цей процес повинні бути долучені приманки і пастки. Все ці дії повинні бути синхронізовані в корпоративних мережах для досягнення результативності з виявлення КА чи дій ЗПЗ.

Під час реалізації обманних дій можуть залучатись приманки і пастки, але можуть і не залучатись. Приманки і пастки можуть бути залучені обманними системами для опрацювання окремих дій в окремих вузлах корпоративних мереж.

Реалізація обманних дій, крім застосування самих обманних технологій, в обманних системах базується на поведінці, яка сформована згідно алгоритму дискретної оптимізації молі і полум'я. При його застосуванні, наприклад, щодо керування приманками і пастками можливим варіантом дії є активізація або переведення в пасивний стан приманок і пасток. Також, частина вузлів корпоративних мереж може бути вимкнена, а певна інша частина може імітувати інтенсивну взаємодію для привертання уваги зловмисників. Крім обманних дій, якими повинні бути наповнені обманні системи, вони повинні самі синтезувати нові дії з використанням базових дій та оцінювати їх ефективність при здійсненні протидії зловмисним впливам, що викликані КА чи діями ЗПЗ. Формування таких нових синтезованих дій може бути здійснено згідно кроків

алгоритму молі і полум'я, а також можуть бути реалізовані в архітектурі обманних систем інші популяційні алгоритми або декілька з подальшим вибором одного з ним в певних станах систем.

Задамо основні кроки методу організації функціонування обманних систем з приманками і пастками в корпоративних мережах.

1. Формування обманних систем з приманками і пастками в корпоративних мережах та забезпечення взаємодії їх розподілених компонентів.

2. Опрацюванні штатних і позаштатних подій в оточуючому середовищі та при взаємодії між компонентами систем та перехід до кроку 3.

3. Виконання визначених функцій з виявлення та протидії КА та ЗПЗ.

4. Вибір наступних кроків обманних систем згідно методу синтезу популяційних алгоритмів в архітектурі обманних систем.

5. Виконання обманних дій та керування приманками і пастками згідно рішень, які визначено на кроці 4.

6. Формування та доповнення обманних систем з приманками і пастками окремо від приманок і пасток набором обманних дій.

7. Формування та доповнення обманних систем приманками і пастками.

Ці кроки не є послідовними. Вся система є розподіленою, тому вони можуть виконуватись паралельно в різних її частинах.

Особливість методу організації функціонування обманних систем з приманками і пастками в корпоративних мережах в тому, що для уникнення реалізації двоцільових атак зловмисниками, суть яких у класифікації об'єктів корпоративних мереж на реальні та хибні, функціонування приманок і пасток в складі обманних систем організовано таким чином, що протягом часу функціонування обманних систем з приманками і пастками зловмисникам ускладнено такі 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. Це, зокрема, дає змогу ускладнити зловмиснику розуміння реальних та хибних об'єктів в корпоративних мережах.

Реалізація популяційних алгоритмів в архітектурі обманних систем, зокрема алгоритму молі і полум'я, при виборі ними наступних кроків 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, а також враховувати потенційну спроможність зловмисників до здійснення двоцільових КА.

Експерименти

Перевірку досягнення мети здійснимо на основі такого експерименту.

Для дослідження алгоритму зміни сервера в розподіленій системі було розгорнуто експериментальне середовище на базі програмного емулятора Cisco Packet Tracer, що відтворює типову інфраструктуру корпоративної мережі середнього підприємства з підвищеними вимогами до безпеки. Досліджувана топологія мережі складалась із чотирьох комутаторів другого рівня моделі Cisco Catalyst 2960-24TT, об'єднаних у ієрархічну структуру типу core-distribution, маршрутизатора Cisco ISR4321 для забезпечення міжмережної взаємодії між віртуальними локальними мережами, та міжмережного екрана Cisco ASA 5505 для сегментації демілітаризованої зони від внутрішніх мереж.

Мережна інфраструктура була сегментована на чотири віртуальні локальні мережі відповідно до функціонального призначення та політик інформаційної безпеки: VLAN 10 призначено для управлінських завдань з адресним простором 192.168.10.0/24 та містить десять робочих станцій (PC0-PC9), VLAN 20 виділено для продуктивних систем з адресацією 192.168.20.0/24 та включає десять робочих станцій (PC10-PC19), VLAN 30 зарезервовано для середовища розробки з діапазоном адрес 192.168.30.0/24 також десятьма робочими станціями (PC20-PC29). Демілітаризована зона DMZ використовує адресний простір 192.168.40.0/24 для розміщення публічних серверів, включаючи HTTP-сервер, поштовий сервер та зовнішній FTP-сервер. Серверна інфраструктура також включає внутрішні сервери DHCP та Internal FTP, розташовані поза DMZ для обслуговування внутрішніх потреб організації. Досліджувану мережну інфраструктуру, у якій здійснювалось проведення експериментів, подано на рис. 4.

Початкове розміщення серверного вузла було здійснено на робочій станції PC18 з IP-адресою 192.168.20.18, що належав до сегмента VLAN 20. Вибір даного вузла обумовлений його центральним розташуванням у топології та типовим навантаженням, характерним для корпоративних розподілених застосунків.

Для кількісної оцінки мережних характеристик між серверним вузлом PC18 та дев'ятьма іншими робочими станціями в мережі було проведено серію систематичних вимірювань з використанням стандартних діагностичних утиліт. Метрика затримки Round Trip Time визначалась за допомогою протоколу ICMP через надсилання послідовності з десяти пакетів розміром 32 байти до кожного цільового вузла з подальшим усередненням отриманих значень часу відгуку. Кількість проміжних вузлів на шляху передачі даних встановлювалась методом трасування маршруту з реєстрацією кожного маршрутизатора, міжмережного екрана або комутатора третього рівня, через які проходить пакет від джерела до призначення.

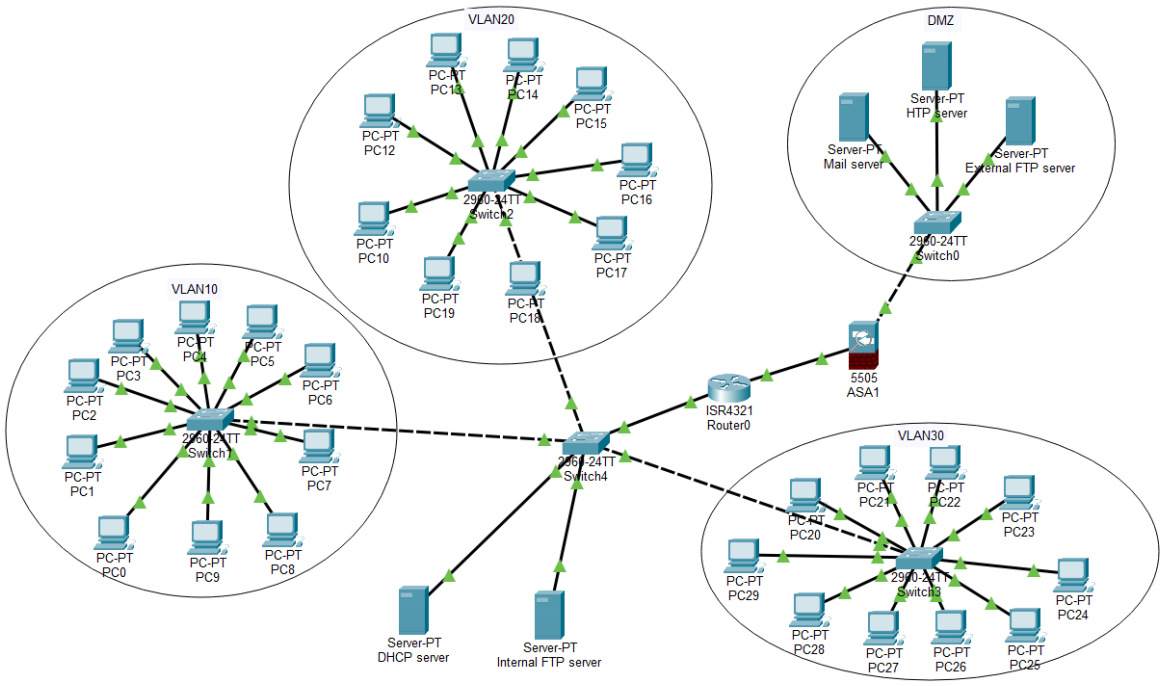


Рис.4. Мережева інфраструктура для проведення експериментів

З метою симуляції типових затримок корпоративної мережі на інтерфейсах міжсегментних з'єднань було застосовано обмеження пропускної здатності шляхом зміни режиму дуплексу з повного (full-duplex) на напівдуплексний (half-duplex), що призводить до збільшення часу передачі даних через необхідність арбітражу доступу до середовища. Додатково на магістральних trunk-портах між комутаторами Switch1, Switch2 та Switch4 швидкість інтерфейсів було знижено зі стандартних 1 Гбіт/с до 100 Мбіт/с, що імітує застаріле обладнання або перевантажені канали в реальних умовах експлуатації. На інтерфейсах міжмережевого екрана Cisco ASA 5505 було введено додаткові затримки на рівні 2-3 мілісекунди для моделювання процесів глибокої інспекції пакетів та обробки правил безпеки, характерних для з'єднань через DMZ.

Результати вимірювань продемонстрували очікувану залежність між топологічною віддаленістю вузлів та значеннями мережних метрик. Для вузлів у межах одного сегмента VLAN 20 середній час відгуку становив від 0.6 до 1.2 мілісекунди при кількості хопів від одного до двох, що відповідає прямій комутації на рівні L2. Міжсегментні з'єднання до вузлів VLAN 10 та VLAN 30 характеризувались RTT у діапазоні 8.5-12.8 мілісекунди та п'ятьма хопами, що обумовлено необхідністю проходження через розподільний комутатор, центральний комутатор Switch4, маршрутизатор ISR4321 та комутатор цільового сегмента. З'єднання до вузлів у демілітаризованій зоні DMZ демонструвало найвищі значення RTT у діапазоні 14.2-18.5 мілісекунди при шести-семи хопах через обов'язкове проходження через міжмережний екран ASA 5505 з додатковою інспекцією трафіку.

Для формалізації задачі вибору оптимального цільового вузла зміни сервера у розподіленій системі було запропоновано комбіновану метрику відстані, що враховує як часові характеристики мережного з'єднання, так і топологічну складність маршруту. Метрика визначалась за формулою:

$$D = \alpha \cdot \left(\frac{RTT}{RTT_{max}}\right) + \beta \cdot \left(\frac{Hops}{Hops_{max}}\right), \quad (6)$$

де D представляє нормалізовану відстань від поточного серверного вузла до потенційного кандидата на зміну, RTT позначає виміряний середній час кругового обігу пакета в мілісекундах, $Hops$ є кількістю транзитних вузлів на маршруті, RTT_{max} та $Hops_{max}$ виступають максимальними значеннями відповідних параметрів у межах досліджуваної мережі для забезпечення нормалізації, а коефіцієнти α та β визначають вагові внески кожної компоненти у підсумкову метрику з умовою $\alpha + \beta = 1$.

У контексті даного дослідження було обрано $\alpha = 0{,}7$ та $\beta = 0{,}3$, що надає пріоритет часовим характеристикам передачі даних над топологічною відстанню, оскільки для більшості розподілених застосунків саме латентність виступає критичним фактором продуктивності.

Було досліджено (рис. 5) два альтернативних варіанти вибору цільового вузла для зміни серверного компонента. Перший варіант передбачав пошук глобального оптимуму шляхом мінімізації метрики D серед усіх доступних вузлів мережі, незалежно від їх сегментної приналежності. За результатами обчислень найменше значення метрики $D = 0{,}158$ було зафіксовано для вузла PC12 з IP-адресою 192.168.20.2 який знаходиться в тому самому сегменті VLAN 20, що й початковий сервер PC18. Така конфігурація забезпечувала RTT на рівні 0.8 мілісекунди та потребувала лише двох хопів для досягнення, що робить цей варіант оптимальним з точки зору мінімізації мережевих накладних витрат.

Другий варіант розглядав ситуацію, коли зміна мала відбутися до альтернативного сегмента внутрішньої мережі з міркувань балансування навантаження або диверсифікації ризиків відмови. У цьому

випадку множина потенційних кандидатів обмежувалася вузлами VLAN 10 та VLAN 30, виключаючи поточний сегмент VLAN 20. Застосування критерію мінімізації до цієї обмеженої множини виявило вузол PC5 з адресою 192.168.10.5 як оптимальний вибір з метрикою $D = 0{,}787$. Цей вузол належить до управлінського сегмента VLAN 10 і характеризувався RTT у 9.2 мілісекунди та п'ятьма хопами, що є найкращим показником серед міжсегментних з'єднань у межах внутрішньої мережі.

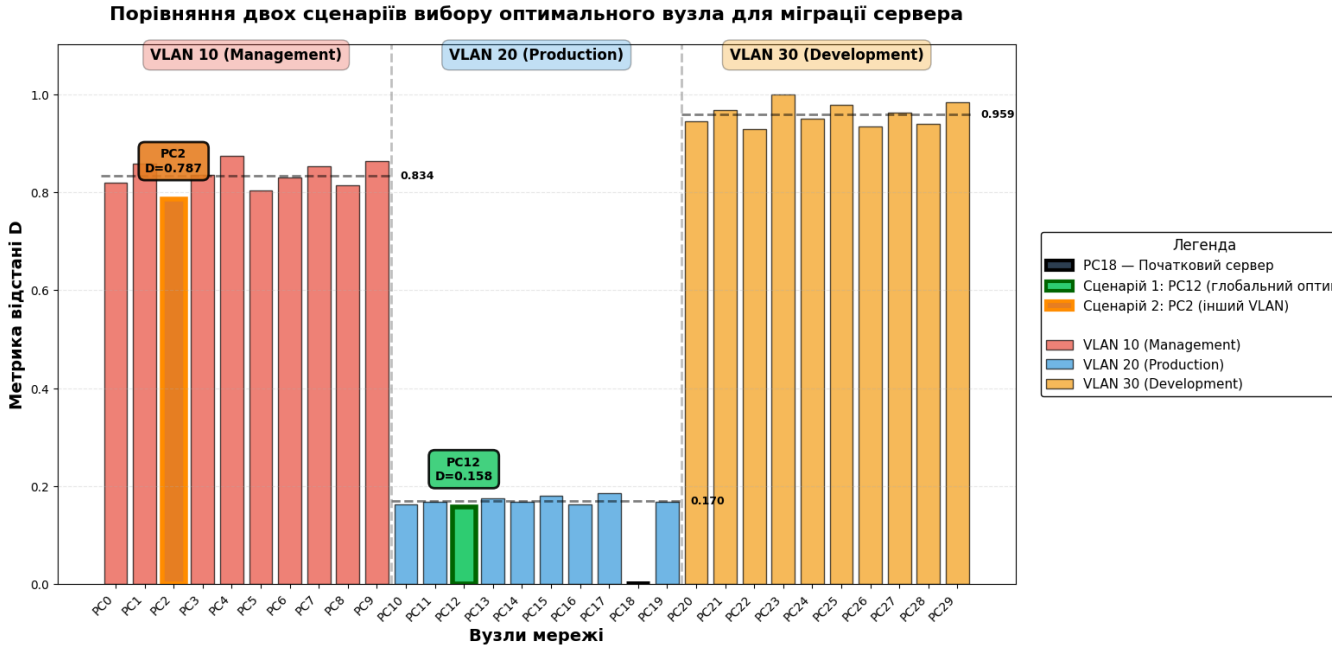


Рис.5. Порівняння двох сценаріїв

Аналіз експериментальних результатів демонструє чітку диференціацію мережевих метрик між сегментами віртуальних локальних мереж. Середня відстань до вузлів VLAN 10 становить 0.834, до VLAN 20 – 0.170 (без урахування самого PC18), а до VLAN 30 – 0.959, що відображає суттєві відмінності у мережевій доступності між сегментами. Виявлено, що внутрішньосегментна міграція забезпечує п'ятикратне зменшення метрики відстані порівняно з міжсегментною (0.158 проти 0.787), що підтверджує критичну важливість топологічного розміщення серверних компонентів для мінімізації латентності. Запропонований підхід на основі комбінованої метрики дозволяє систематизувати процес вибору цільового вузла, забезпечуючи баланс між оптимізацією продуктивності через мінімізацію мережевих затримок та стратегічними вимогами до розподілу навантаження і відмовостійкості системи шляхом міжсегментної диверсифікації.

Висновки

Розроблено метод організації функціонування обманних систем з приманками і пастками в корпоративних мережах, суть якого в тому, що для уникнення реалізації двоцільових атак зловмисниками функціонування приманок і пасток в складі обманних систем організовано таким чином, що протягом часу функціонування обманних систем з приманками і пастками зловмисникам ускладнено такі 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. Реалізація алгоритму молі і полум’я в архітектурі обманних систем при виборі ними наступних кроків 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, а також враховувати потенційну спроможність зловмисників до здійснення двоцільових КА.

Напрямами подальших досліджень є розроблення архітектури обманних систем, їх позиціонування в корпоративних мережах та зв’язок з приманками та пастками.

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. Kashtalian A., Ścisło Ł., Rucki R., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Control and Decision-Making in Deceptive Multi-Computer Systems Based on Previous Experience for Cybersecurity of Critical Infrastructure. *Applied Sciences*, 2025. Vol. *15*(22), 12286. DOI: https://doi.org/10.3390/app152212286

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. Dahiya M., Nitin N., Dahiya D. Intelligent Cyber Security Framework Based on SC-AJSO Feature Selection and HT-RLSTM Attack Detection. *Appl. Sci.* 2022, *12*, 6314. https://doi.org/10.3390/app12136314

8. Aslan O., Ozkan-Okay M., Gupta D. Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access* 2021, *9*, 83252–83271.

9. Connor M., Michail O., Spirakis P. On the Distributed Construction of Stable Networks in Polylogarithmic Parallel Time. *Information* 2021, *12*, 254. https://doi.org/10.3390/info12060254

10. Dai F., Hossain M.A., Wang Y. State of the Art in Parallel and Distributed Systems: Emerging Trends and Challenges. *Electronics* 2025, *14*, 677. https://doi.org/10.3390/electronics14040677

11. Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor, S.; Gorbovy O. Borusiewicz A. Cyber Security Risk Modeling in Distributed Information Systems. *Appl. Sci.* 2023, *13*, 2393. https://doi.org/10.3390/app13042393

12. Pinto S.J., Siano P., Parente M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies* 2023, *16*, 1651. https://doi.org/10.3390/en16041651

13. Ayele E.D., Gonzalez J.F., Teeuw W.B. Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. *Sensors* 2024, *24*, 854. https://doi.org/10.3390/s24030854

14. Zhou B., Sun B., Zang T., Cai Y., Wu J., Luo H. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. *Entropy* 2023, *25*, 47. https://doi.org/10.3390/e25010047

15. Wang X., Shi B., Fang Y. Distributed Systems for Emerging Computing: Platform and Application. *Future Internet.* 2023, *15*, 151. https://doi.org/10.3390/fi15040151

16. Acevedo-Iles M., Romero-Quete D., Cortes C.A. A Distributed Coordination Approach for Enhancing Protection System Adaptability in Active Distribution Networks. *Energies* 2024, *17*, 4338. https://doi.org/10.3390/en17174338

17. Kurttisi A., Dogan K.M., Gruenwald B.C. A Novel Distributed Adaptive Controller for Multi-Agent Systems with Double-Integrator Dynamics: A Hedging-Based Approach. *Electronics.* 2024, *13*, 1142. https://doi.org/10.3390/electronics13061142

18. Li Q., Zeng F. Enhancing Software Architecture Adaptability: A Comprehensive Evaluation Method. *Symmetry* 2024, *16*, 894. https://doi.org/10.3390/sym16070894

19. Ayedh M. A.T., Wahab A.W.A., Idris M.Y.I. Enhanced Adaptable and Distributed Access Control Decision Making Model Based on Machine Learning for Policy Conflict Resolution in BYOD Environment. *Appl. Sci.* 2023, *13*, 7102. https://doi.org/10.3390/app13127102

20. Brouillet M., Georgiev G.Y. Modeling and Predicting Self-Organization in Dynamic Systems out of Thermodynamic Equilibrium: Part 1: Attractor, Mechanism and Power Law Scaling. *Processes.* 2024, *12*, 2937. https://doi.org/10.3390/pr12122937

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. Kashtalian A., Ścisło Ł., Rucki R., Lysenko S., Sachenko A., Savenko B., Savenko O., Nicheporuk A. Control and Decision-Making in Deceptive Multi-Computer Systems Based on Previous Experience for Cybersecurity of Critical Infrastructure. *Applied Sciences*, 2025. Vol. *15*(22), 12286. DOI: https://doi.org/10.3390/app152212286

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. Dahiya M., Nitin N., Dahiya D. Intelligent Cyber Security Framework Based on SC-AJSO Feature Selection and HT-RLSTM Attack Detection. *Appl. Sci.* 2022, *12*, 6314. https://doi.org/10.3390/app12136314

8. Aslan O., Ozkan-Okay M., Gupta D. Intelligent behavior-based malware detection system on cloud computing environment. *IEEE Access* 2021, *9*, 83252–83271.

9. Connor M., Michail O., Spirakis P. On the Distributed Construction of Stable Networks in Polylogarithmic Parallel Time. *Information* 2021, *12*, 254. https://doi.org/10.3390/info12060254

10. Dai F., Hossain M.A., Wang Y. State of the Art in Parallel and Distributed Systems: Emerging Trends and Challenges. *Electronics* 2025, *14*, 677. https://doi.org/10.3390/electronics14040677

11. Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor, S.; Gorbovy O. Borusiewicz A. Cyber Security Risk Modeling in Distributed Information Systems. *Appl. Sci.* 2023, *13*, 2393. https://doi.org/10.3390/app13042393

12. Pinto S.J., Siano P., Parente M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies* 2023, *16*, 1651. https://doi.org/10.3390/en16041651

13. Ayele E.D., Gonzalez J.F., Teeuw W.B. Enhancing Cybersecurity in Distributed Microgrids: A Review of Communication Protocols and Standards. *Sensors* 2024, *24*, 854. https://doi.org/10.3390/s24030854

14. Zhou B., Sun B., Zang T., Cai Y., Wu J., Luo H. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. *Entropy* 2023, *25*, 47. https://doi.org/10.3390/e25010047

15. Wang X., Shi B., Fang Y. Distributed Systems for Emerging Computing: Platform and Application. *Future Internet.* 2023, *15*, 151. https://doi.org/10.3390/fi15040151

16. Acevedo-Iles M., Romero-Quete D., Cortes C.A. A Distributed Coordination Approach for Enhancing Protection System Adaptability in Active Distribution Networks. *Energies* 2024, *17*, 4338. https://doi.org/10.3390/en17174338

17. Kurttisi A., Dogan K.M., Gruenwald B.C. A Novel Distributed Adaptive Controller for Multi-Agent Systems with Double-Integrator Dynamics: A Hedging-Based Approach. *Electronics.* 2024, *13*, 1142. https://doi.org/10.3390/electronics13061142

18. Li Q., Zeng F. Enhancing Software Architecture Adaptability: A Comprehensive Evaluation Method. *Symmetry* 2024, *16*, 894. https://doi.org/10.3390/sym16070894

19. Ayedh M. A.T., Wahab A.W.A., Idris M.Y.I. Enhanced Adaptable and Distributed Access Control Decision Making Model Based on Machine Learning for Policy Conflict Resolution in BYOD Environment. *Appl. Sci.* 2023, *13*, 7102. https://doi.org/10.3390/app13127102

20. Brouillet M., Georgiev G.Y. Modeling and Predicting Self-Organization in Dynamic Systems out of Thermodynamic Equilibrium: Part 1: Attractor, Mechanism and Power Law Scaling. *Processes.* 2024, *12*, 2937. https://doi.org/10.3390/pr12122937