КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.970
УДК 004.056:004.75

Цирканюк Діана Андріївна
аспірантка кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна
ORCID 0000-0002-9422-8617
d.tsyrkaniuk.asp@kubg.edu.ua

РОЗШИРЕНА ГІБРИДНА МОДЕЛЬ З УРАХУВАННЯМ РИЗИКІВ ТА КООПЕРАТИВНИХ СТРАТЕГІЙ ЗАХИСТУ ХМАРНОГО СЕРЕДОВИЩА

Анотація. У статті розроблено та теоретично обґрунтовано розширену гібридну модель кооперативно-еволюційного розподілу задач у хмарних обчислювальних системах (ХОС) з урахуванням динамічного рівня кіберризиків та кооперативних стратегій захисту. Запропонована модель інтегрує багатокритеріальну еволюційну оптимізацію на основі модифікованого алгоритму NSGA-II з теоретико-ігровими підходами, включаючи кооперативні, неантагоністичні та коаліційні ігри. Вперше введено динамічну функцію ризику λ(t), яка змінюється в часі відповідно до стохастичних, марковських або еволюційних моделей, що дозволяє адекватно відображати адаптивну природу сучасних кіберзагроз та залежність ризику від стану системи, навантаження, історії атак і дій захисника. Розроблено гнучку адаптивну стратегію захисника, яка в реальному часі реагує на поточний рівень ризику шляхом перерозподілу задач, міграції на менш вразливі вузли, посилення захисту критичних компонентів та оптимізації використання ресурсів безпеки. Окрім традиційних критеріїв оптимізації – продуктивності (час виконання), вартості та рівня безпеки – вперше введено критерій вигоди коаліції як окремий об'єкт оптимізації, що відображає синергетичний ефект співпраці між різними захисними компонентами чи організаціями в умовах мультихмарних або розподілених середовищ. Проведено комп'ютерне моделювання на синтетичних даних, що імітують реальну хмарну інфраструктуру. Отримано множину Парето-оптимальних рішень у чотиривимірному просторі цільових функцій. Якість отриманого фронту Парето оцінено за стандартними метриками. Результати свідчать про високу диверсифікацію рішень та ефективне відображення компромісів між конфліктуючими критеріями, а також підтверджують можливість досягнення значної коаліційної вигоди за рахунок помірного зростання ризику чи вартості. Запропонований метод CoopEvo-CloudSec демонструє високу адаптивність до змінного ризикового профілю хмарного середовища, забезпечуючи баланс між продуктивністю, економічною ефективністю, безпекою та колективною вигодою від співпраці захисників. Модель описана у вигляді формалізованих математичних виразів, псевдокоду та блок-схеми алгоритму, що робить її придатною для подальшої програмної реалізації та практичного застосування в реальних хмарних інфраструктурах.

Ключові слова: хмарні обчислення, розподіл ресурсів, кібербезпека, теорія ігор, кооперативні ігри, коаліційні ігри, еволюційна оптимізація, NSGA-II, динамічний ризик, багатокритеріальна оптимізація.

ВСТУП

Розподіл хмарних ресурсів дедалі частіше поєднує еволюційну оптимізацію з теоретико-ігровими або явними моделями ризику для спільного управління продуктивністю, вартістю, справедливістю та безпекою.

Найсучасніші підходи, що найбільше узгоджуються з «кооперативно-еволюційним розподілом з ризиком», поєднують багатоцільові еволюційні алгоритми з теоретико-ігровими або явними моделями ризику для компромісу між часом виконання, вартістю

та безпекою. Кооперативна коеволюція ефективна для декомпозиції складних рішень щодо розподілу та для навчання евристики планування, тоді як теоретико-ігрові шари фіксують справедливість, ціноутворення та поведінку зловмисника та захисника. Відкриті виклики включають масштабованість до дуже великих хмар, багатші моделі реальних ризиків та тіснішу інтеграцію поведінки користувачів та угод про рівень обслуговування з еволюційними контролерами.

Постановка проблеми. Стаття присвячена розробці математичної моделі розподілу обчислювальних задач у хмарній інфраструктурі з урахуванням основних параметрів, що визначають результативність та стійкість роботи ХОС [1]. У запропонованій моделі розглядаємо формалізацію процесу прийняття рішень щодо призначення задач на доступні обчислювальні вузли (ОВ) з огляду на три взаємопов'язані параметри – забезпечення високої продуктивності, оптимізація вартості використання ресурсів, мінімізація ризиків, пов'язаних з кіберзагрозами для хмарного середовища (ХС). Запропонована модель є гібридною, адже поєднує засоби багатокритеріальної оптимізації з положеннями теорії ігор. Це дозволяє, комплексно враховувати як внутрішні параметри ХОС, так і потенційні загрози з боку зловмисника (хакера чи хакерів). У межах даної статті поетапно подано формалізацію ігрової взаємодії, математичне визначення функцій втрат, ризиків та критеріїв оптимізації, а так саме відповідні обмеження, що описують припустимі конфігурації ХОС. Запропонована модель становить основу для подальшої реалізації інтелектуальної системи для завдання управління хмарними обчислювальними ресурсами з метою підвищення їх стійкості до загроз та оптимального використання.

Аналіз останніх досліджень і публікацій. У попередньому дослідженні [2] було розглянуто гібридну модель, яка поєднує теорію ігор «зловмисник-захисник» з модифікованим NSGA-II для розподілу завдань, мінімізуючи ризик компрометації вузла, час обробки та вартість, явно моделюючи агресивність зловмисника та адаптивний захист. Планування хмарних робочих процесів розглядається як трицільова проблема (час, вартість, ризик безпеки), що вирішується за допомогою кластерного коеволюційного алгоритму, який використовує кілька взаємодіючих популяцій та стратегії інтенсифікації/диверсифікації, перевершуючи кілька базових рівнів EA та RL [3]. Кооперативна коеволюція та генетичне програмування використовуються для вивчення правил розміщення контейнерів в інтернеті, які спільно розподіляють контейнери → віртуальні машини та віртуальні машини → фізичні машини, значно зменшуючи енергоспоживання, реагуючи на моделі робочого навантаження [4]. Кооперативні еволюційні обчислення також застосовуються до мобільних периферійних обчислень на базі БПЛА для спільної оптимізації черг розвантаження, затримки та енергії за обмежених ресурсів [5], а також для спільної максимізації корисності постачальника та клієнта в хмарних центрах обробки даних [6]. Велике дослідження показує, що еволюційні обчислення (GA, PSO, ACO, коеволюція) широко використовуються для управління хмарними ресурсами, оскільки проблеми є масштабними, динамічними та NP-складними; жодна окрема метаевристика не є домінантною, а проекти повинні бути специфічними для проблеми [7]. Огляди розподілу ресурсів на периферії/в тумані підкреслюють зростаюче використання теорії ігор, аукціонів та машинного навчання для обробки конкуренції, якості обслуговування (QoS) та невизначеності в хмарному континуумі [8–10].

МЕТОДИКА ДОСЛІДЖЕННЯ

Розглядаємо задачу синтезу ігрової моделі оцінки ризику, яка опишіть стратегічну поведінку зловмисника, орієнтовану на максимізацію шкоди, та захисника, що прагне мінімізувати втрати від потенційних атак на ХС. На другому етапі виконано оцінку ризику, яка здобута в наслідок цієї взаємодії. Далі її інтегруємо у багатокритеріальну постановку задачі розподілу задач за допомогою еволюційного алгоритму NSGA-II. У сукупності модель дозволяє отримати множину компромісних рішень, що відображають різні сценарії балансування між критеріями ефективності, вартості й безпеки ХОС.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Як розкрито у [2] у ХС загрози КІБ мають рухливий характер, адаптуються до поточних змін інфраструктури та активності користувачів. Статичні моделі ризику, засновані на фіксованих значеннях параметрів, не можуть повною мірою відобразити складність нових атак. Крім того, захисні стратегії мають адаптуватися до поточного рівня ризику, обмеженості ресурсів, а також до перспективи кооперації між підсистемами безпеки (або навіть між різними хмарними провайдерами в умовах мультихмарності).

Тому в рамках дослідження вважаємо доцільним розширити гібридну модель, додавши:

– варіативність параметра ризику $\lambda(t)$, який змінюємо в часі або в залежності від сценарію атаки на ХС;

– гнучку стратегію захисника $\pi^D(t)$, що обирає рішення в залежності від спостережуваного ризику;

– коаліційні або/та неантагоністичні ігрові моделі, що дозволяють моделювати співпрацю між захисниками, або обмежені цілі атакувальника, відмінні від повної деструкції.

Позначимо $\lambda(t) \in [0,1]$ – коефіцієнт ризику в момент часу t.

Залежність для розрахунку ризику запишемо так:

$$R(t) = \sum_{i=1}^{N} \lambda(t) \cdot p_i(x_i, t), \quad (1)$$

де $p_i(x_i, t)$ – ризик атаки на ресурс i у момент часу t; x_i – розподіл обчислювальних задач на ресурсі i.

Параметр $\lambda(t)$ – змінюємо відповідно до однієї з моделей:

– стохастичної $\lambda(t) \sim u[\lambda_{\min}, \lambda_{\max}]$,

– марковської, де дискретні стани ризику з матрицею переходів P_λ,

– еволюційної, коли тренд зростання або зниження $\lambda(t)$ знаходится в залежності від минулих атак.

Підкреслимо, що у розширеній моделі розподілу обчислювальних ресурсів з урахуванням кіберзагроз ризик не є стабільною величиною. Він міняється в залежності від низки факторів, пов’язаних як з діями атакувальника, так і з особливостями поведінки користувачів, навантаженням на систему, станом її компонентів, та навіть з історією попередніх атак. Саме тому в поточному параграфі $\lambda(t)$ вводиться як функція часу. Або

навіть ширше, як функція стану системи. Це дозволяє на наступних етапах дослідження моделювати реалістичні сценарії розвитку подій при атаках на ХС.

В умовах підвищеного навантаження на хмарну інфраструктуру, скажімо, під час запуску великого онлайн-заходу або періоду масової звітності у фінансовій сфері система є більш вразливою до атак. Це стається через перевантаження ресурсів і зниження результативності засобів виявлення вторгнень. У такому випадку параметр $\lambda(t)$ має зростати, сигналізуючи про підвищення ризику. І навпаки, після впровадження нових компонентів верифікації доступу або після завершення пікового навантаження, ризик знижується. Величина $\lambda(t)$ теж зменшиться. Параметр $\lambda(t)$ відображає поточний стан безпекової ситуації в ХС.

Так само, слід зазначити, що у попередньому параграфі параметр λ інтерпретувався як інтенсивність атак або агресивність дій атакувальника. Інакше кажучи параметр λ в моделі фактично описував частоту атак або силу тиску з боку зловмисника. Параметр λ був елементом ігрової моделі, яка моделює стратегії нападника у вигляді потоку або частоти загроз.

У поточному параграфі, де йдеться про ризик, $\lambda(t)$, цей параметр вже виступає як узагальнена характеристика рівня ризику в системі, який включає не лише інтенсивність атак, але й низку інших чинників. Передусім, таких як вразливість ХС, неефективність її захисту, наявність активних експлойтів, внутрішніх збоїв, тощо.

Підкреслимо, що це не суперечність. А є розширенням інтерпретації параметра λ в рамках більш загальної моделі. Зокрема, у базовій (ігровій) моделі параметр λ інтерпретований локально. Приміром, як стратегічний параметр гравця (нападника), що визначає його поточну поведінку. У розширеній же моделі $\lambda(t)$ вже набуває системного змісту і вважається функцією часу або стану, яка акумулює вплив як зовнішніх загроз (дій нападника або початкове значення λ), так і внутрішніх умов (вразливості, навантаження, відповідь захисника).

Для опису того, як саме змінюється $\lambda(t)$, доцільно розглянути декілька моделей його поведінки. Стохастична модель визначає, що ризик змінюється випадковим чином у певних межах, відображаючи ситуації, коли точну природу загрози неможливо передбачити, а атаки мають ознаки випадкових вторгнень. Передусім, у відкритих публічних хмарах може відбуватись хаотичне сканування портів або масові фішингові кампанії, які виникають незалежно від стану конкретної системи. У цьому випадку $\lambda(t)$ трактуємо (обчислюємо) як випадкову величину з певного інтервалу. А стратегія захисника повинна бути адаптованою до невизначеності.

Інша ситуація – коли ХС має справу з більш структурованими атаками. Скажімо, з боку постійно діючого суб'єкта таргетованих атак (або APT). Таку атаку реалізують зазвичай за певними шаблонами [11, 12]. У такому випадку дійовою є Марковська модель зміни ризику, де система переходить із одного стану в інший з певними ймовірностями [13, 14]. Наприклад, з «низького» ризику у «середній», або з «середнього» у «високий» ризик, залежно від кількості несанкціонованих спроб входу, виявлених у певний проміжок часу. Таке моделювання дозволить включати в систему передбачення майбутнього ризику на ґрунті оцінки поточного стану і допомагає побудувати оптимальні стратегії захисту ХС наперед.

Нарешті, еволюційна модель $\lambda(t)$ визначає, що ризик змінюється поступово в часі, відображаючи або накопичення загроз, або їхній спад у результаті результативної роботи захисту [15, 16]. Після виявлення нової вразливості у віртуалізаційному шарі (скажімо у гіпервізорі), $\lambda(t)$ починає зростати, оскільки очікується поява експлойтів у відкритому доступі. Протягом кількох днів рівень ризику зростає, поки не буде виправлено

вразливість або впроваджено відповідні патчі. У такій моделі $\lambda(t)$ є функцією, що залежить не тільки від зовнішніх умов, але й від дій самої системи. Або від її спроможності до виявлення та реагування. Таки моделі забезпечують гнучкість у відображенні довгострокових трендів кіберзагроз.

Тому моделювання ризику через параметр $\lambda(t)$ дозволяє нам на цьому етапі досліджень адаптувати інтелектуальну систему до різних сценаріїв розвитку подій. Залежно від властивостей середовища – чи то обмежена інформація про зловмисника, чи детерміновані шаблони його поведінки, чи тривалі зміни ризиків – відповідна модель $\lambda(t)$ дозволяє приймати оптимальні рішення щодо розподілу ресурсів, пристосування стратегії захисту ХС та формування ефективного опору кіберзагрозам. Зазначимо, що урахування величини ризику через змінну функцію $\lambda(t)$ дозволило нам перейти від спрощеної (статичної) оцінки загроз до більш реалістичного сценарію, де ризик формувався під впливом численних факторів, включаючи дії зловмисників, вразливість ХС, обмеження ресурсів та час реакції. Перехід до адаптивної інтерпретації параметра ризику природно висуває нові вимоги до поведінки захисної сторони. У таких умовах фіксована або наперед задана стратегія захисту виявиться недостатньо дієвою. Першою чергою це стосувалося випадків коли атаки на ХС стають все більш складними або змінюють свою природу в часі. Тому наступним вирішальним елементом розширеної гібридної моделі є формалізація стратегії захисника, яка враховує поточний рівень ризику, обмеження ресурсів та прогнозовану поведінку нападника для перерозподілу задач, посилення захисту критичних компонентів і мінімізації потенційних втрат.

Рішення захисника в момент часу t позначаємо як $\pi^D(t)$, де

$$\pi^D(t) = \arg\max_{\pi \in \Pi} U_D(\pi, \lambda(t), C), \tag{2}$$

де U_D – доцільність стратегій захисника ХС, яка бере до уваги ризик $R(t)$, продуктивність системи $P(t)$ та вартість C.

Формально

$$U_D = w_1 \cdot P(t) - w_2 \cdot R(t) - w_3 \cdot C(\pi), \tag{3}$$

де w_1, w_2, w_3 – вагові коефіцієнти.

Вагові коефіцієнти w_1, w_2, w_3 визначаємо на підставі:

– політики безпеки підприємства. Передусім, критичні бази даних які компанії розтасовують у ХС отримують більший w_i, ніж допоміжні хмарні сервіси;.

– класифікації інформаційних активів. Вузли ХС, що обробляють конфіденційну інформацію, одержують вищий пріоритет;

– аналізу впливу. Як, приклад, коефіцієнт w_i пропорційний до потенційних втрат у разі успішної атаки на ХС.

– емпіричних даних. Скажімо, виходячи з історії інцидентів у хмарній інфраструктурі, деякі типи задач потенційно можуть бути частіше атакованими. Інакше кажучи, їх вага підвищується.

Як обґрунтовано у [17], доцільним є запровадження гнучкої стратегії захисника, яка бере до уваги зміну рівня загроз у часі, обмеження на ресурси захисту, та пріоритетність тих чи інших вузлів або обчислювальних задач. Метою є своєчасна

переорієнтація ресурсів безпеки відповідно до змін параметра агресивності атакуючого $\lambda(t)$ та розподілу ризиків у системі.

Формально, варіативну стратегію захисника представимо як функцію прийняття рішень [18]:

$$A(t) = \arg\max_{a(t)\in A}\left[\sum_{i=1}^{n} w_i \cdot \phi_i\left(x_i(t), \lambda(t), R_i(t)\right)\right], \quad (4)$$

де $A(t)$ – вектор варіативних дій захисника в момент часу (t). Насамперед, зміна маршрутів задач, посилення захисту, міграція задач на менш ризиковані вузли ХС; A – множина припустимих дій; w_i – ваговий коефіцієнт, що відображає значення (або критичність ресурсу/вузла ХС; ϕ_i – функція дієвості захисних дій ХС, що враховує значення ризику $R_i(t)$, агресивність атакуючого $\lambda(t)$ та поточний стан обчислювального вузла ХС $x_i(t)$; $R_i(t)$ – оцінка ризику для вузла в момент часу (t), що отримано з попереднього етапу (оцінка ризику на базі результатів гри); $x_i(t)$ – стан задачі/вузла – завантаження, залишок ресурсів, критичність функцій, які виконує задача.

Відмітимо, що якщо попередні судження описували протистояння між атакуючим і захисником як гру з нульовою сумою, де виграш одного точно дорівнює втратам іншого, то в реальних сценаріях взаємодія сторін складніша. Насамперед у багатокористувацьких або мультиорганізаційних ХС виникають ситуації, де захисники різних компонентів системи змушені кооперувати свої ресурси для підвищення загальної безпеки, тоді як атакуючі можуть діяти не індивідуально, а в рамках узгоджених стратегій або навіть коаліцій.

За таких обставин класична модель гри стає надто спрощеною для адекватного моделювання реальних загроз і стратегій реагування на них.

Саме тому, розгляд кооперативних або неантагоністичних моделей дозволив в рамках дослідження змістити фокус з жорсткої конкуренції до більш реалістичної взаємодії. В такій взаємодії можливе часткове узгодження інтересів сторін. Або хоча б існування спільного простору рішень, в рамках якого оптимізаційна задача не обов’язково має єдиного переможця. Як-от у випадках, коли атакуючий не має за мету повне виведення ХС з ладу, а прагне отримати вигоду у формі витоку обмеженої кількості даних або незначного контролю, можлива часткова рівновага, яку доцільно моделювати в рамках неантагоністичних біматричних ігор.

Аналогічно, захисники можуть формувати коаліції. Це можуть бути коаліцій як формальні (між компаніями-партнерами), так і динамічні (між компонентами кластерної інфраструктури ХС). А це вимагає врахування аспектів розподілу спільного виграшу, створення довіри між захисниками та оптимального об'єднання ресурсів.

Формально це вимагає переходу від класичної матриці виграшу до біматричної моделі зі змінною вигодою, де кожен учасник отримує свою вигоду відповідно до обраної стратегії та стратегії супротивника, і ця вигода не є обов’язково симетричною чи взаємовиключною. Така модель дозволяє описувати взаємодію у вигляді пари функцій виграшу:

$$\left(U_D(s_D, s_A), U_A(s_D, s_A)\right), \quad (5)$$

де s_D, s_A – відповідно, стратегії захисника та атакуючого, а функції виграшу можуть залежати від зовнішніх змінних. Як-от рівень ризику, стан системи чи доступність ресурсів.

Це розширення, на нашу думку, слушне в умовах багатокритеріальної оптимізації, коли використовуємо алгоритм, як у нашому випадку алгоритм NSGA-II. Адже останній дозволяє знайти множину Парето-оптимальних стратегій не лише в сенсі максимізації/мінімізації класичних метрик (надійності, вартості, продуктивності), а й з урахуванням взаємодії між гравцями, які мають неідентичні й не завжди протилежні інтереси.

Тож резюмуючи наші судження, зазначимо, що включення кооперативної або неантагоністичної ігрової моделі в дослідження не лише підвищує рівень реалізму математичного опису загроз у хмарній системі, але й дає змогу нам змогу інтегрувати її з багатоцільовою оптимізацією. Подібна інтеграція дозволяє, на нашу думку, сформувати стратегії, які не лише дієві в умовах конфлікту, а й гнучко адаптуються до ситуацій, коли співпраця або компроміс між сторонами – бажаний або навіть необхідний варіант рівноваги.

В результаті отримуємо більш загальну гібридну модель, яка включає як елементи оптимального розподілу ресурсів (через NSGA-II), так і моделі прийняття рішень у середовищі зі змінними, але не обов'язково конфліктними інтересами.

Тоді подамо ігрову модель так:

Нехай:

– захисник – гравець D,

– атакувальник (зловмисник / (зловмисники для кооперативної ігри)) – гравець A,

– Π^D, Π^A – множини стратегій, відповідно.

Тоді у кооперативному або неантагоністичному сценарії маємо систему рівнянь:

$$U_D(\pi^D, \pi^A) = f\big(P(t), R(t), C(\pi^D)\big), \quad (6)$$

$$U_A(\pi^D, \pi^A) = g(Control, Visibility, Cost_A), \quad (7)$$

де f, g – відповідні функції вигоди сторін. Та гравці не обов'язково мають повністю протилежні цілі.

Якщо в ХС декілька захисників $D_1, D_2, \ldots, D_m$, належить використати ігри з коаліціями. Таки ситуації є типовими для розподілених хмарних архітектур, де різні компоненти інфраструктури (сервери, віртуальні машини, сервіси, мережеві вузли та ін.) належать або управляються різними адміністративними доменами. У таких випадках загроза атаки торкнеться кількох захисників одночасно, і виникає потреба у кооперації, щоб знизити ризик, зменшити загальні втрати або ефективніше розподілити ресурси на протидію.

Наведемо невеликий приклад ситуації для використання ігор з коаліціями, див. табл. 1.

Таблиця 1

Ілюстрація формування коаліції захисників у хмарній інфраструктурі

Параметр	Опис	Випадок для трьох хмарних провайдерів (U1, U2, U3)
Учасники коаліції	Суб'єкти, що об'єднують ресурси для спільного захисту ХС	U1 (відеосервіси), U2 (опрацювання даних), U3 (аналітика)
Виграш коаліції $v(S)$	Зменшення загального ризику внаслідок співпраці.	—
Внесок кожного учасника коаліції	Розподіл виграшу згідно з принципом справедливості (напр., значення Шеплі [19, 20])	—
Ресурси коаліції	Спільне використання інструментів захисту, даних про загрози тощо	U1 надає систему DDoS-захисту, U2 – моніторинг вразливостей, U3 – алгоритми аналітики для виявлення аномалій
Ілюстрація реального застосування	Кооперація для протидії DDoS-атаці на спільний освітній портал	Атака на портал зберігає його доступність через перерозподілення навантаження між U1, U2, U3

Відповідно до прикладу, який розглянуто у табл. 1, уявімо собі ХС, в якому розгорнуто об'єднану платформу освітніх послуг, що надається трьома університетами (назвемо їх U1, U2, U3). Кожен з університетів має свою локальну інфраструктуру в хмарі, але й відкриває частину своїх ресурсів спільному освітньому порталу. Параметр U1 обслуговує навчальний контент і відеосервіси. Тоді як U2 відповідає за обробку персональних даних студентів. А U3 виконує аналітичну опрацювання запитів та рекомендацій. Кожен із цих вузлів має своїх захисників, які можуть в автономному режимі будувати системи безпеки. Як, приклад, здійснювати налаштування брандмауерів, IDS/IPS, шифрування даних тощо. Проте в разі скоординованої DDoS, EDoS -атаки, або таргетованого відпливу персональних даних через вузол U2, усі три учасники втрачають репутацію, і навіть якщо конкретна атака торкнулася лише одного вузла, наслідки розповсюджуються на всю хмарну платформу. Логічно, що у такій ситуації стає вигідним сформувати коаліцію захисників, які обмінюються інформацією про загрози в реальному часі, та розподіляють ресурси захисту залежно від рівня загрози на кожному вузлі та координують стратегії реагування. Тоді у термінах теорії ігор [21] таку взаємодію моделюємо як коаліційну гру. В подібній грі учасники формують коаліції з метою максимізації колективної вигоди або мінімізації загальних втрат [22]. При цьому виникають задачі розподілу виграшу всередині коаліції. Інакше кажучи хто скільки отримає від запобігання атаці, і як оцінити внесок кожного захисника.

Найперше, якщо завдяки коаліції уникнено збитків у розмірі 100000 у.о., доречно з'ясувати, яку частину цієї «вигоди» приписати кожному з вузлів. Це доцільно зробити насамперед через значення Шеплі (Shapley value) [19, 20], що оцінює внесок кожного гравця в коаліцію.

Тоді виграш коаліції $S \subseteq \{D_1, D_2, \dots, , D_m\} - v(S)$, визначаємо як зменшення ризику:

$$v(S) = \Delta R_S = R_{\text{без}S} - R_{\text{з}S}, \quad (8)$$

де $R_{\text{без}S}$ – параметр, який використовуємо у задачах розрахунку виграшу коаліції в іграх з переданим виграшом. Параметр $R_{\text{без}S}$ використовуємо для оцінки внеску коаліції до загального виграшу або втрат системи; $R_{\text{з}S}$ – виграш системи або рівень безпеки, який

досягнутий без участі коаліції S. Інакше кажучи, це базовий результат системи (як-от, рівень виявлення атак, зменшення втрат, показник ризику), коли дана група захисників не бере участі у спільних діях або діє автономно; $R_{\text{без}S} - R_{\text{з}S}$ – внесок коаліції S у загальну безпеку ХС. Власне, ця різниця $v(S)$ є виграш коаліції, який потім використовуємо для розрахунку справедливого розподілу вигоди між її учасниками (насамперед, за допомогою значення Шеплі [19, 20]).

При використанні багатокритеріальних еволюційних алгоритмів, NSGA-II (або NSGA-III), ми зможемо оцінювати ефективність різних коаліцій як частину множини можливих стратегій захисників ХС, включати виграш коаліції $v(S)$ як один із критеріїв оптимізації (разом із вартістю, надійністю, продуктивністю). Але це вже чотири критерія тому потрібно задіяти NSGA-II. Так саме варте в подальшому розглядати утворення коаліцій як еволюційно обумовлений процес, де домінантними залишаються ті стратегії взаємодії, що забезпечують найвищу вигоду ХС.

Враховуючи всі судження, опишемо формальну подачу загальної цілі оптимізації в розширеній моделі.

Потрібно знайти розподіл задач $X = (x_i)$, та оптимальні стратегії $\pi^D(t)$, що максимізують векторну функцію:

$$\begin{cases} Maximize\ F_1 = \mathbb{E}[P(t)]; \\ Minimize\ F_2 = \mathbb{E}[R(t)]; \\ Minimize\ F_3 = \mathbb{E}[C(t)]; \\ Maximize\ F_4 = v(S), \quad \text{(коаліційна вигода)}, \end{cases} \tag{9}$$

при обмеженнях:

$$\begin{gathered} x_i(t) \in [0, x_i^{max}], \\ \sum_i x_i(t) \le R^{total}(t), \\ \pi^D(t) \in \Pi, \text{ залежно від } \lambda(t). \end{gathered} \tag{10}$$

Як і минулого разу наведемо псевдокод для розширеної гібридної моделі.

1: Ініціалізувати множину задач T та множину вузлів N
2: Ініціалізувати початкову популяцію рішень P(0)
3: Задати початкове значення параметра λ для кожного вузла
4: ***while*** *(не досягнуто критерію зупинки)*
5: Оцінити стан системи: A(t), λ(t), R(t)
6: Оновити значення λ(t) відповідно до вибраної моделі (Марковської / еволюційної)
7: Застосувати гнучку стратегію захисника:
8: Моніторинг активності атак
9: Перерозподіл задач між вузлами
10: ***if*** *(виявлено коаліцію атакуючих або захисників)*
11: Провести аналіз вигод RбезS та RзS для кожної коаліції
12: Оновити структуру взаємодії (кооперативна/неантагоністична гра)
13: Виконати NSGA-II: відбір, кросовер, мутація
14: Оцінити кожне рішення за критеріями F1–F4
15: Зберегти поточну популяцію та значення метрик (IGD, Spacing, HV)
16: ***end while***
17: Вивести фінальне Парето-оптимальне рішення

Блок-схема алгоритму для розширеної гібридної моделі з урахуванням ризиків та кооперативних стратегій захисту ХС наведена на рис. 2.

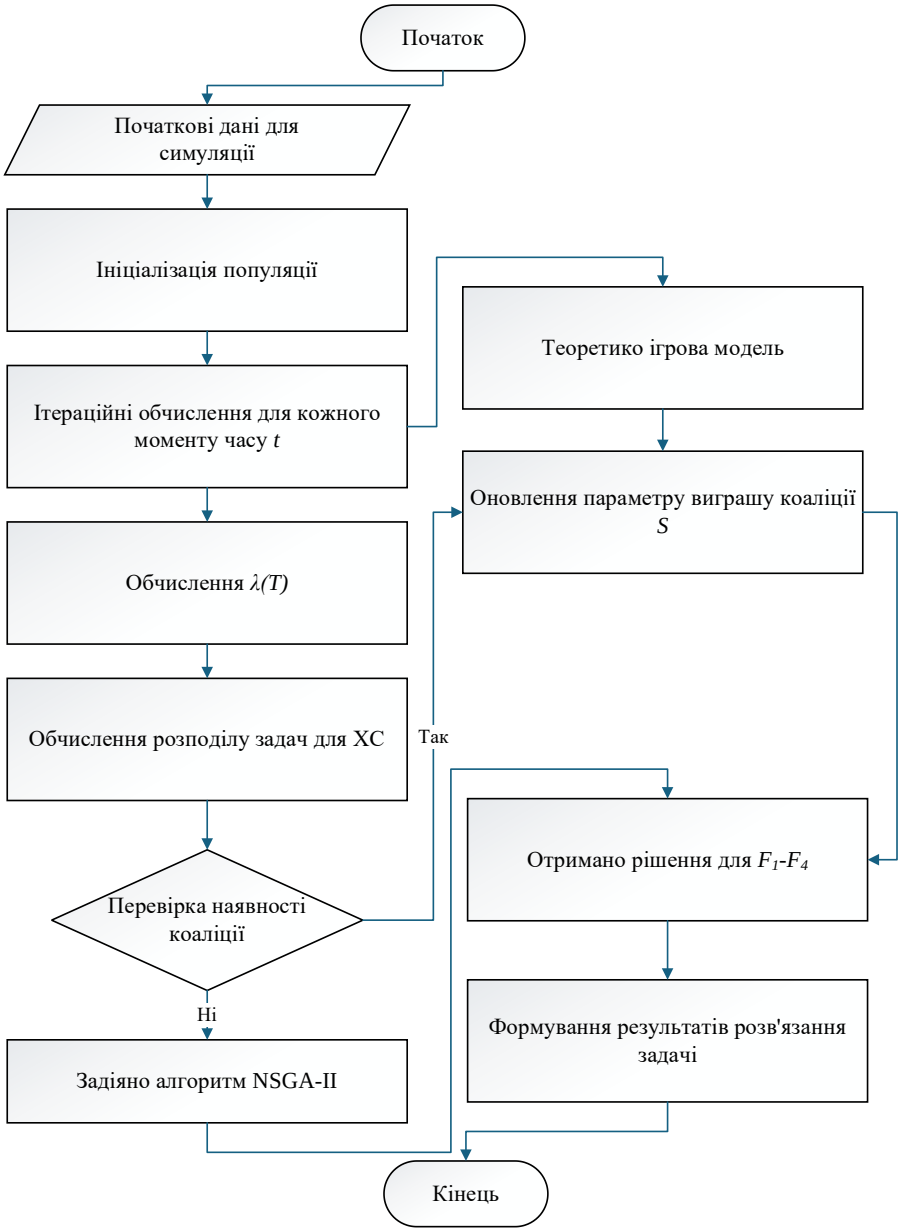

Рис. 2. Блок-схема алгоритму для розширеної гібридної моделі з урахуванням ризиків та кооперативних стратегій захисту ХС

А далі наведемо пояснення для основних фрагментів псевдокоду.

В рядках 1–3 ініціалізуємо структуру задач та обчислювальної інфраструктури, та встановлюємо початкове значення агресивності λ для кожного вузла ХС.

У рядку 5 фіксуємо поточний стан ХС, включно з рівнем атак, ризиком та параметром λ.

У 6 рядку відповідно до обраної моделі ризику (Марковської або еволюційної), значення λ змінюється в часі, відображаючи зміну поведінки атакуючих.

В рядках 7–9 реалізуємо варіативну (гнучку) стратегію захисника. Скажімо, при зростанні $\lambda(t)$ або зменшенні доступності ресурсів, задачі перерозподіляються на менш уразливі вузли ХС.

В рядках 10–12 перевіряємо, чи виникли коаліції гравців. Якщо так, то тоді використовуємо модель з обчисленням виграшів коаліцій для прийняття стратегічних рішень. Це дозволить змоделювати реальні сценарії співпраці між захисниками ХС.

В рядку 13 застосовуємо алгоритм NSGA-II для пошуку Парето-оптимального розподілу задач.

В рядку 14 виконуємо оцінку кожного розв’язку. Це реалізовано за чотирма критеріями (8).

В рядку 15 здійснюємо збереження результатів. Результати зберігаються разом з обчисленими метриками якості, що дозволяє провести постсимуляційний аналіз.

В рядку 17 формуємо вихід моделі – множину оптимальних розв'язків, графіки змін $\lambda(t)$, ризику та розподілу задач.

Тому блок-схема, представлена на рис. 4, відтворює логіку функціонування розширеної гібридної моделі оптимізації розподілу обчислювальних ресурсів у ХС з урахуванням ризику, варіативної поведінки захисника та кооперативної взаємодії між суб’єктами захисту. Згідно з послідовністю етапів, представлених на рис. 4, процес розпочинаємо з ініціалізації початкових даних симуляції. Ці дані включають параметри задач, ресурсів хмарної інфраструктури, та початкові характеристики популяції розв'язків, що будуть надалі оброблятися у межах алгоритму багатокритеріальної оптимізації, відповідно до моделі (1)–(10).

Після цього запускаємо ітеративний цикл, у межах якого здійснюємо обчислення змінного параметра ризику $\lambda(t)$. У подальшому модель (1)–(10) виконує перевірку наявності коаліційної взаємодії між захисними агентами. У випадку, якщо коаліція відсутня, система залучає алгоритм NSGA-II для пошуку Парето-оптимальних рішень відповідно до сформульованих критеріїв $F_1 - F_4$.

Якщо ж коаліція між захисниками все-таки сформована, розгортання процесу переходить до інтеграції теоретико-ігрової моделі. Ця модель дозволяла враховувати вигоди колективної взаємодії для критеріїв $F_1 - F_4$. У цьому випадку здійснюємо оновлення параметру виграшу коаліції, що віддзеркалює внесок кожного з учасників до спільної мети захисту ХС. На підставі отриманих розв’язків, незалежно від того, чи були вони сформовані за допомогою NSGA-II, чи в рамках кооперативної моделі, реалізуємо підсумкову оцінку значень цільових функцій та формуємо остаточні результати розв’язання задачі.

Зазначимо, що аналіз теоретичної складності запропонованої гібридної моделі доцільно проводити з урахуванням основних її структурних компонентів, кожен з яких має власну алгоритмічну природу. Наша модель (1)–(10) включає обчислення рівня ризику $\lambda(t)$, реалізацію кооперативної взаємодії учасників системи на ґрунті теоретико-ігрового підходу, та багатокритеріальну оптимізацію з використанням еволюційного алгоритму NSGA-II. Розглянемо часову (обчислювальну) та просторову складності кожної складової окремо.

Обчислення рівня $\lambda(t)$, з урахуванням зміни поточних загроз та стану захисних механізмів, передбачає аналіз вхідних даних, таких як історія інцидентів, рівень захищеності ресурсів та актуальний стан ХС. У випадку дискретизації часу з кроком Δt, складність оцінювання функції ризику на кожному кроці є $O(n)$, де n – кількість активних задач у ХС.

Загальна складність обчислення ризику протягом періоду моделювання з T дискретними моментами часу оцінюємо як $O(T \cdot n)$.

Просторова складність обмежується збереженням тимчасових послідовностей значень параметрів задач і станів ресурсів, що становить $O(n \cdot T)$.

Побудова коаліційної взаємодії між захисниками ХС базувалася на формуванні множини припустимих коаліцій, розрахунку виграшу кожної коаліції та визначенні рівноважного розподілу прибутку. У випадку наявності (m) захисників, кількість можливих коаліцій зростає експоненційно і становить 2^m. Для кожної коаліції варто виконати оцінювання виграшу, що базувалася на стані системи та рівні загроз. Складність цієї компоненти в загальному випадку оцінюємо як $O(2^m \cdot c)$, де c – вартість обчислення виграшу однієї коаліції.

Просторова складність визначалася як $O(2^m)$, для збереження виграшів або стратегій усіх коаліцій.

Блок багатокритеріальної оптимізації, реалізований за допомогою алгоритму NSGA-II, має складність $O(P^2)$, на кожній ітерації, де P – розмір популяції. Це пов'язано з необхідністю виконання операцій сортування за фронтами Парето. Тоді при загальній кількості ітерацій G, повна часова складність алгоритму становить $O(G \cdot P^2)$. А просторова складність є $O(P \cdot d)$, де d – розмірність вектору розв'язків (у даній моделі – чотири критерії $F_1 - F_4$).

Узагальнюючи, повна обчислювальна складність моделі на одному етапі симуляції (для фіксованого моменту часу) оцінено так:

$$O(n + 2^m \cdot c + G \cdot P^2), \tag{11}$$

а відповідна просторова складність:

$$O(n + 2^m + P \cdot d). \tag{12}$$

Ці оцінки свідчать про прийнятну складність реалізації моделі для середніх масштабів ХС, маємо такі параметри: $m < 10$, $n \sim 10^2 - 10^3$, $P \sim 100$, $G \sim 100$.

В умовах масштабування, та збільшення кількості коаліційних учасників захисту ХС, виникне потреба у використанні апроксимаційних або евристичних компонент для зменшення експоненційної частини у коаліційній взаємодії.

Для запропонованого в поточному параграфі моделі (1)–(10) була проведена симуляція з урахуванням ризиків та кооперативних стратегій захисту ХС, див. рис. 3.

Експериментальне дослідження ефективності запропонованого гібридного підходу проведено на синтетичних даних, згенерованих для імітації роботи хмарної інфраструктури. Дані для симуляції наведено у табл. 2.

В ході дослідження виконано 300 поколінь оптимізації з використанням модифікованого алгоритму NSGA-II, що дозволило отримати 100 Парето-оптимальних розв'язків, див. рис. 3 (візуалізовано у терміналі IDE PyCharm).

Якість знайденого фронту оцінювалася за допомогою трьох вирішальних метрик:

– гіпероб'єму (Hypervolume – HV);

– зворотної генераційної відстані (Inverted Generational Distance – IGD);

– метрики рівномірності розподілу (Spread).

Синусоїдальна компонента $0{,}2 + 0{,}1 \cdot sin\left(\frac{2\pi t}{100}\right)$ імітує циклічність кіберзагроз, пов'язаних із плановими навантаженнями на систему. Параметр t інтегрує інформацію про розподіл задач. Це в моделі дозволяє брати до уваги їхню взаємозалежність. Результати такої симуляції подано на рис. 4–6.

Таблиця 2

Параметри синтетичних даних для моделювання розподілу обчислювальних задач у хмарній системі

Параметр	Діапазон значень / значення	Пояснення
Кількість обчислювальних задач	10 (фіксовано)	Визначає загальну кількість задач, що підлягають розподілу по вузлах хмарної інфраструктури
Кількість ресурсних вузлів	5 (фіксовано)	Відповідає за кількість доступних обчислювальних вузлів у хмарній системі
Рівень ризику вузлів	[0,1, 0,5] (рівномірний розподіл)	Характеризує вразливість кожного вузла до кібератак. Генеруємо окремо для кожного вузла
Час обробки задач	[5, 20] (рівномірний розподіл)	Час виконання кожної задачі на конкретному вузлі (умовні одиниці). Формує матрицю задачі×вузол
Вартість опрацювання	[10, 50] (рівномірний розподіл)	Витрати на виконання задачі на обраному вузлі. Формує матрицю задачі×вузол
Користь від коаліції	[0,5, 2,0] (рівномірний розподіл)	Додаткова перевага від спільної роботи задач на одному вузлі. Унікальне значення для кожного вузла
Ризик	$0{,}2 + 0{,}1 \cdot sin\left(\frac{2\pi t}{100}\right)$	Функція, що моделює часову зміну рівня загроз у системі, де t – сумарний індекс задач
Розмір популяції	100 (фіксовано)	Кількість індивідуумів у популяції генетичного алгоритму за одне покоління
Кількість поколінь	300 (фіксовано)	Максимальна кількість ітерацій алгоритму оптимізації
Ймовірність схрещування	0,85	Імовірність застосування оператора схрещування до пари індивідуумів
Ймовірність мутації	0,15	Імовірність застосування оператора мутації до індивідуума

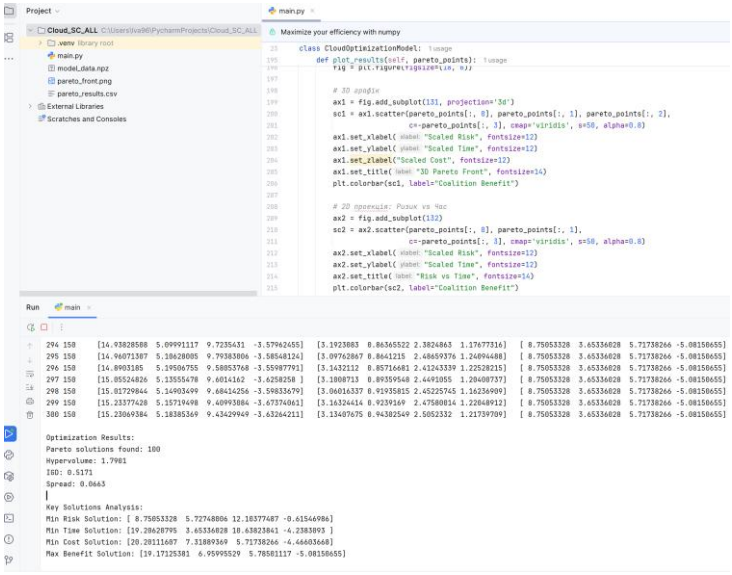

Рис. 3. Симуляція для запропонованої розширеної гібридної моделі з урахуванням ризиків та кооперативних стратегій захисту ХС

Метрика зворотної генераційної відстані зафіксувала значення IGD = 0,5171. Це відтворює середню відстань між знайденими рішеннями та точками референсного фронту. Хоч цей показник і не досяг ідеального рівня, він свідчить про прийнятну близькість до теоретично оптимальних розв’язків, приймаючи до уваги складність задачі з чотирма конфліктними критеріями. Зазначимо, що генерація референсного фронту виконувалась шляхом випадкового пошуку, що могло обмежити точність порівняння. А крім того ми використовували синтетичний набір даних для попереднього етапу дослідження, де головним була перевірка працездатності нашої моделі (1)–(10).

Рівномірність розподілу розв’язків уздовж Парето-фронту оцінювалась за допомогою метрики Spread, яка показала значення 0,0663, див. рис. 3. Даний результат свідчить про відчутну диверсифікацію знайдених розв’язків. А це досить ґрунтовний аргумент на користь подальшого вибору оптимальної конфігурації захищеної ХС із мінімізованим рівнем ризику для безпеки. Рівномірний розподіл гарантує, що суб’єкт прийняття рішень матиме широкий вибір варіантів із різними балансами критеріїв.

Детальний аналіз головних розв’язків, візуалізованих на рис. 3 виявив певні закономірності. Рішення з мінімальним ризиком (8,7505) демонструє вагомий компроміс у вигляді підвищеної вартості (12,1038) та обмеженої користі від коаліції (0,6155).

На противагу цьому, варіант із мінімальним часом виконання (3,6534) супроводжується підвищеним рівнем ризику (19,2062). А це підкреслює фундаментальний потенційний конфлікт між продуктивністю та безпекою в хмарних системах. Також при симуляції одержано розв'язок із найбільшою вигодою коаліції (5,0815). Цей розв'язок реалізує синергію між складовими інфраструктури шляхом помірного збільшення ризику (19,1713) та часу опрацювання (6,9599).

Виявлені під час комп’ютерної симуляції компроміси зайвий раз підтверджують теоретичні передумови дослідження щодо неможливості одночасного досягнення оптимуму за всіма критеріями. Сильна негативна кореляція між рівнем ризику та іншими показниками наочно проявилася у варіантах з мінімальною вартістю (5,7174) та максимальною користю коаліції. У цьому випадку зменшення витрат супроводжувалося зростанням загроз безпеці.

Проведений обчислювальний експеримент заклав основу для подальших досліджень на реальному наборі даних.

Окрім виводу результатів моделювання у консолі IDE PyCharm, отримано декілька графічних результатів, які наведено на рис. 4–6.

На рис. 4 представлено візуалізацію результатів багатокритеріальної оптимізації розподілу ресурсів у ХС, отриманих за допомогою генетичного алгоритму NSGA-II із урахуванням сукупної вигода від коаліції (Coalition Benefit), який підлягав максимізації. Графік демонструє фінальну множину недомінованих розв'язків, які утворюють так званий фронт Парето. Графічно це чотиривимірний простір цільових функцій, спроєктований на тривимірну діаграму розсіювання для наочного аналізу. Кожна точка на графіку відповідає одному оптимальному рішенню щодо розподілу обчислювальних завдань між доступними ресурсами.

Осі абсцис, ординат та аплікат представляють три основні критерії, що підлягали мінімізації:

– масштабований ризик (Scaled Risk);
– масштабований час виконання (Scaled Time);
– масштабована вартість (Scaled Cost).

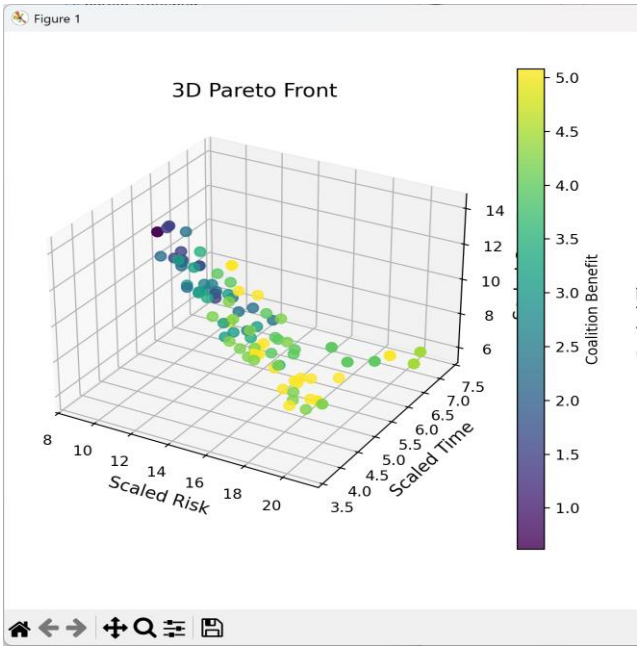

Рис. 4. Результати багатокритеріальної оптимізації: тривимірна поверхня фронту Парето

Четвертий критерій – сукупна вигода від коаліції (Coalition Benefit – який підлягав максимізації) візуалізовано за допомогою кольорової шкали. Тепліші кольори (жовтий) відповідають вищим значенням вигоди, тоді як холодніші (фіолетовий, синій) – нижчим.

Сукупність отриманих точок формує поверхню, яка наочно відповідає компромісу між конкуруючими цілями (критеріями). Розбір візуалізації показує, що рішення з мінімальними значеннями ризику, часу та вартості, розташовані ближче до початку координат. Ці точки характеризуються нижчою вигодою від коаліції (представлені синіми та зеленими точками). І навпаки, для досягнення максимальної вигоди від коаліційного об'єднання ресурсів захисту ХС (жовті точки) слід йти на поступки, погоджуючись на вищий рівень системного ризику для ХС, довший час виконання завдань або більші фінансові витрати на захист. Отриманий фронт Парето надає особі, що приймає рішення (ОПР), набір оптимальних, але різних за своїми характеристиками альтернатив. Жодне з цих рішень не є найкращим за інше за всіма критеріями одночасно. Ці в результаті дозволяють ОПР гнучко обирати стратегію розподілу ресурсів ХС залежно від поточних пріоритетів. Отже це – мінімізація ризиків для критичних операцій. Чи максимізація продуктивності та економічної ефективності для стандартних завдань.

На рис. 5 подано двовимірну проекцію отриманого фронту Парето. Цей моделювання результат деталізує взаємозв'язок між двома критеріями оптимізації – масштабованим ризиком (Scaled Risk) та масштабованим часом (Scaled Time). Окремі маркери відображають недоміновані конфігурації розподілу ресурсів ХС.

Третій суттєвий вимір, вигода від коаліції (Coalition Benefit), інтегрований у візуалізацію через колірне кодування. Це зручно, бо дозволяє відразу оцінити додатковий параметр, не перевантажуючи графік. Як бачимо, діаграма на рис. 6 демонструє обернену залежність між ризиком та часом. Така ситуація є доволі типовою для багатокритеріальних задач подібного класу. Спостерігаємо виражену тенденцію – стратегії, що мінімізують час виконання завдань (розташовані в нижній частині графіка),

які пов'язані з вищим рівнем сукупного ризику. Водночас найбільш безпечні конфігурації ХС, що відповідають мінімальним значенням ризику, вимагають більших на 10–15% часових затрат на виконання.

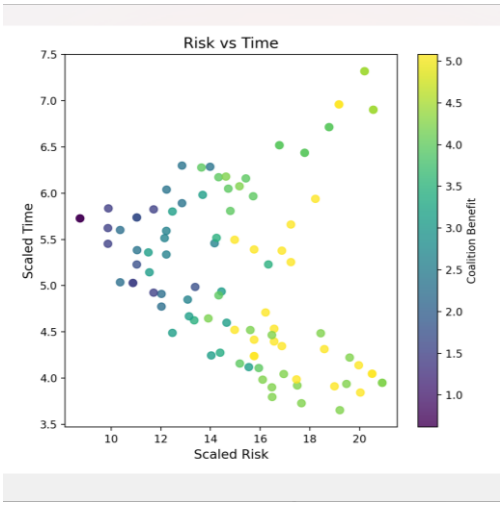

Рис. 5. Двовимірна проекція фронту Парето

Розбір колірного розподілу маркерів на рис. 5 надає ОПР глибше розуміння складних взаємозв'язків розглянутих у моделі (1)–(10) критеріїв $F_1 - F_4$. Найбільш вигідні з точки зору коаліційної взаємодії рішення (жовті маркери) переважно концентруються в області підвищеного ризику. Але з помірним або низьким часом виконання завдань у ХС. Натомість, найменш вигідні рішення (фіолетові маркери) відповідають найбезпечнішим, але водночас і найповільнішим варіантам розподілу. Отримані при симуляції результати показують антагоністичні особливості досліджуваних критеріїв $F_1 - F_4$ і слугують практичним інструментом для ОПР.

Рис. 6 розкриває співвідношення між економічними та безпековими аспектами оптимізації, фокусуючись на критеріях масштабованого ризику (Scaled Risk) та масштабованої вартості (Scaled Cost). Кожен елемент отриманої множини недомінованих рішень зображений як точка на двовимірній площині. Застосування колірної градієнтної заливки для параметра «вигода від коаліції» (Coalition Benefit) дозволяє ОПР одночасно оцінювати й третій вимір ефективності.

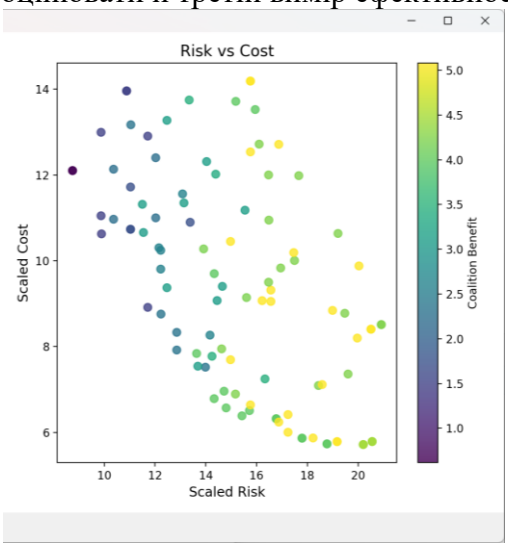

Рис. 6. Співвідношення між ризиком та вартістю в просторі оптимальних рішень

ISSN 2663 - 4023

Рис. 7 представляє пряму залежність між цільовим показником ефективності – коаліційною вигодою (Coalition Benefit) та ключовим обмежуючим фактором – масштабованим ризиком (Scaled Risk).

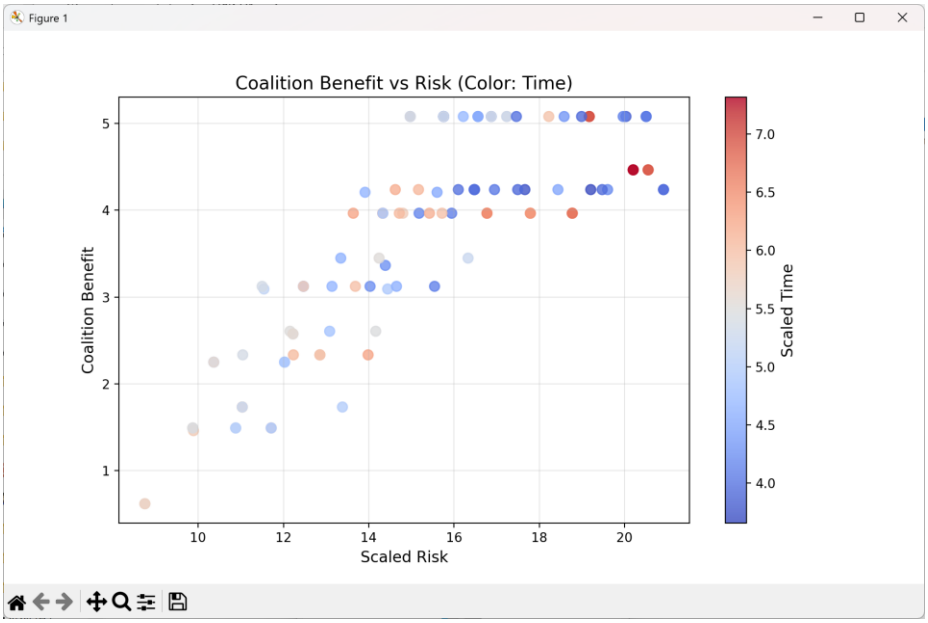

Рис. 7. Залежність коаліційної вигоди від ризику з урахуванням часових витрат

На відміну від попередніх графіків, ця діаграма ставить у центр аналізу результатів нашої комп'ютерної симуляції саме кінцеву вигоду від оптимізації розподілу завдані у ХС із урахуванням мінімізації ризику. Третій критерій, масштабований час (Scaled Time), інтегрований як додатковий інформаційний шар за допомогою колірної палітри, де сині відтінки відповідають меншим часовим витратам, а червоні – більшим.

Графічна картина наведена на рис. 7 на свідчить про наявність вираженої позитивної кореляції між двома основними осями. Зростання рівня прийнятого ризику зумовлює чітку тенденцію до збільшення сукупної вигоди від коаліції. Водночас відзначимо, що ця залежність не є лінійною. Тобто приріст вигоди є швидким на початкових рівнях ризику, після чого спостерігаємо ефект насичення, де подальше збільшення ризику дає все менший приріст вигоди від коаліції захисту ХС. Інформація, що передано кольором, вносить суттєві нюанси в цю картину. Вона демонструє, що досягнення максимальних значень коаліційної вигоди (верхній правий кут) є «найдорожчим» не лише з точки зору ризику, але й часу.

Це підтверджено концентрацією червоних точок у цій зоні. З іншої точки зору, найбільш швидкі рішення (сині точки) розподілені по всьому спектру ризиків. Але, як правило, таки результати не дозволяють досягти найвищих показників вигоди. Підкреслимо, що цей аналітичний зріз результатів нашої симуляції є підґрунтям для стратегічного планування безпеки ХС, адже він дозволяє ОПР виявити «точки перегину», за якими подальше прийняття ризику стає невиправданим через незначне зростання вигоди та суттєве збільшення часу виконання.

Додатково представлена картина дає ОПР можливість формулювати складні комбіновані стратегії. Скажімо, доцільно обирати найкраще за вигодою рішення в рамках припустимого часового лагу. Подібні комбіновані стратегії , суттєві для сервісів ХС із підвищеними вимогами до оперативності.

ОБГОВОРЕННЯ

Метод поєднав в собі інструментарій багатокритеріальної еволюційної оптимізації (на підставі алгоритму NSGA-II) та кооперативної ігрової моделі, і врахуванні ступеню ризику безпеки ХС у часі. На відміну від наявних підходів, відмінностями методу є формалізація компоненти ризику $\lambda(t)$ у моделі розподілу задач, введення критерію коаліційної вигоди як одного з об'єктів оптимізації, та підтримка кооперативних стратегій між ресурсами ХС. Запропонований метод дозволив не лише збалансувати критерії безпеки ХС, продуктивності та вартості, але й забезпечив пристосування до змінного ризикового профілю ХС.

Розроблений метод є узагальненням і розвитку класичних підходів до управління ресурсами в хмарних інфраструктурах. А його реалізація забезпечує гнучку архітектуру захисної поведінки. Запропоновані математичні моделі слід адаптувати до різних сценаріїв, притаманних для ХС та ІТ-систем в цілому.

Крім того, буде розглянуто методику проведення обчислювальних експериментів, яка включатиме:

– побудову тестових сценаріїв;

– вибір параметрів симуляції;

– використання метрик якості для оцінки результатів (вже розглянуті Hypervolume, IGD, Spacing).

Подобний підхід у сукупності дозволить оцінити комплексно результативність і універсальність методу CoopEvo-CloudSec в умовах для хмарних систем компаній та організацій.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В статті запропоновано адаптивний механізм реалізації стратегії захисника, що змінює розподіл завдань залежно від рівня ризику та активності атак. Вперше враховано можливість кооперації між захисниками ХС і введено поняття виграшу коаліції для оцінки доцільності об'єднання.

Об'єднано всі моделі в єдину гібридну модель, описано її у вигляді псевдокоду та блок-схеми. Доведено, що запропонований підхід є гнучким, кооперативно орієнтованим і багатокритеріальним, що забезпечує його наукову новизну та практичну цінність. Сформульовано новий метод кооперативно-еволюційного розподілу ресурсів у ХС з урахуванням ризику (CoopEvo-CloudSec). Його реалізацію, симуляцію та експериментальну перевірку.

Подальші дослідження будуть спрямовані на узагальнений алгоритм реалізації запропонованого методу CoopEvo-CloudSec, та здійснено розгорнуте симуляційне моделювання поведінки системи на ґрунті даних підприємств різних сфер.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Михайлів, В. І. (2015). Експериментальні дослідження інформаційної технології для захисту даних у хмарних обчислювальних системах. *Актуальні проблеми автоматизації та інформаційних технологій, 19*, 52–66.
2. Цирканюк, Д. (2025). Модель розподілу обчислювальних задач у хмарній інфраструктурі з урахуванням продуктивності, вартості та безпеки. *Кібербезпека: освіта, наука, техніка, 4(28)*, 619–632. https://doi.org/10.28925/2663-4023.2025.28.836

3. Qin, S., Pi, D., Shao, Z., & Xu, Y. (2023). A Cluster-based Cooperative Co-Evolutionary Algorithm for Multiobjective Workflow Scheduling in a Cloud Environment. *IEEE Transactions on Automation Science and Engineering, 20(3)*, 1648–1662. https://doi.org/10.1109/tase.2022.3183681
4. Tan, B., , H., Mei, Y., & Zhang, M. (2020). A Cooperative Coevolution Genetic Programming Hyper-Heuristics Approach for On-Line Resource Allocation in Container-Based Clouds. *IEEE Transactions on Cloud Computing, 10(3)*, 1500–1514. https://doi.org/10.1109/tcc.2020.3026338
5. Goudarzi, S., Soleymani, S., Wang, W., & Xiao, P. (2023). UAV-Enabled Mobile Edge Computing for Resource Allocation Using Cooperative Evolutionary Computation. *IEEE Transactions on Aerospace and Electronic Systems, 59*, 5134–5147. https://doi.org/10.1109/taes.2023.3251967
6. Goudarzi, P., Hosseinpour, M., & Ahmadi, M. (2020). Joint Customer/Provider Evolutionary Multi-objective Utility Maximization in Cloud Data Center Networks. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 45(2)*, 479–492. https://doi.org/10.1007/s40998-020-00381-x
7. Guzek, M., Bouvry, P., & Talbi, E.-G. (2015). A Survey of Evolutionary Computation for Resource Management of Processing in Cloud Computing. *IEEE Computational Intelligence Magazine, 10(2)*, 53–67. https://doi.org/10.1109/mci.2015.2405351
8. Atwal, S., Singh, D., & Chhabra, A. (2025). Resource Allocation Strategies for Edge and Fog Computing in the Cloud Continuum. In *2025 Int. Conf. on Intelligent Control, Computing and Communications (IC3)*, 208–213. https://doi.org/10.1109/ic363308.2025.10957263
9. Du, J., Jiang, C., Benslimane, A., Guo, S., & Ren, Y. (2021). SDN-based Resource Allocation in Edge and Cloud Computing Systems: An Evolutionary Stackelberg Differential Game Approach. *IEEE/ACM Transactions on Networking, 30(4)*, 1613–1628. https://doi.org/10.1109/tnet.2022.3152150
10. Fan, W., Zhao, L., Liu, X., Su, Y., Li, S., Wu, F., & Liu, Y. (2024). Collaborative Service Placement, Task Scheduling, and Resource Allocation for Task Offloading With Edge-Cloud Cooperation. *IEEE Transactions on Mobile Computing, 23(1)*, 238–256. https://doi.org/10.1109/tmc.2022.3219261
11. Choi, J., Choi, C., Lynn, H. M., & Kim, P. (2015). Ontology based APT Attack Behavior Analysis in Cloud Computing. In *2015 10th Int. Conf. on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp. 375–379). IEEE. https://doi.org/10.1109/bwcca.2015.69
12. Alshaikh, A., Alanesi, M., Yang, D., & Alshaikh, A. (2023). Advanced Techniques for Cyber Threat Intelligence-based APT Detection and Mitigation in Cloud Environments. In *Int. Conf. on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023)* (Vol. 12718, pp. 147–157). SPIE. https://doi.org/10.1117/12.2681627
13. Шабала, Є., & Корнійчук, Б. (2024). Методологія оцінювання безпеки IoT на промислових об'єктах. *Управління розвитком складних систем, 60*, 146–155. https://doi.org/10.32347/2412-9933.2024.60.146-155
14. Стефурак, О. Р., Тихонов, Ю. О., Лаптєв, О. А., & Зозуля, С. А. (2020). Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації. *Сучасний захист інформації, 2*, 19–26. https://doi.org/10.31673/2409-7292.2020.021926
15. Li, B., Chen, Y., Huang, S., Yao, R., Xia, Y., & Mei, S. (2019). Graphical Evolutionary Game Model of Virus-based Intrusion to Power System for Long-Term Cyber-Security Risk Evaluation. *IEEE Access, 7*, 178605–178617. https://doi.org/10.1109/access.2019.2958856
16. Zhang, H., Tan, J., Liu, X., Huang, S., Hu, H., & Zhang, Y. (2022). Cybersecurity Threat Assessment Integrating Qualitative Differential and Evolutionary Games. *IEEE Transactions on Network and Service Management, 19(3)*, 3425–3437. https://doi.org/10.1109/tnsm.2022.3166348
17. Höfer, C. N., & Karagiannis, G. (2011). Cloud Computing Services: Taxonomy and Comparison. *Journal of Internet Services and Applications, 2(2)*, 81–94. https://doi.org/10.1007/s13174-011-0027-x
18. Li, P., & Yang, X. (2019). On Dynamic Recovery of Cloud Storage System under Advanced Persistent Threats. *IEEE Access, 7*, 103556–103569. https://doi.org/10.1109/access.2019.2932020
19. Winter, E. (2002). Chapter 53 The shapley value. In Handbook of Game Theory with Economic Applications (pp. 2025–2054). Elsevier. https://doi.org/10.1016/s1574-0005(02)03016-3
20. Faigle, U., & Kern, W. (1992). The Shapley Value for Cooperative Games under Precedence Constraints. *International Journal of Game Theory, 21*, 249–266.
21. Голованенко, М. (2012). Застосування теорії кооперативних ігор для розвитку корпоративної соціальної відповідальності. *Україна: аспекти праці, 2*, 47–50.
22. Павлов, І. М., & Толюпа, С. В. (2014). Аналіз підходів моделювання процесів прийняття рішень при проектуванні систем захисту інформації. *Сучасний захист інформації, 2*, 96–104.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Diana A. Tsyrkaniuk
Ph.D. student of the Department of Information and
Cyber Security named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9422-8617
d.tsyrkaniuk.asp@kubg.edu.ua

ADVANCED HYBRID MODEL WITH RISK-BASED AND COOPERATIVE CLOUD SECURITY STRATEGIES

Abstract. The article develops and theoretically justifies an extended hybrid model of cooperative-evolutionary distribution of tasks in cloud computing systems, taking into account the dynamic level of cyber risks and cooperative protection strategies. The proposed model integrates multi-criteria evolutionary optimization based on the modified NSGA-II algorithm with game-theoretic approaches, including cooperative, non-antagonistic and coalition games. For the first time, a dynamic risk function λ(t) is introduced, which varies in time according to stochastic, Markov or evolutionary models, which allows us to adequately reflect the adaptive nature of modern cyber threats and the dependence of risk on the state of the system, load, attack history and defender actions. A flexible adaptive defender strategy is developed, which responds in real time to the current level of risk by redistributing tasks, migrating to less vulnerable nodes, strengthening the protection of critical components and optimizing the use of security resources. In addition to the traditional optimization criteria – performance (execution time), cost and security level – the coalition benefit criterion was introduced for the first time as a separate optimization object, reflecting the synergistic effect of cooperation between different protective components or organizations in multi-cloud or distributed environments. Computer modeling was performed on synthetic data simulating real cloud infrastructure. A set of Pareto-optimal solutions was obtained in the four-dimensional space of objective functions. The quality of the resulting Pareto front was assessed using standard metrics. The results indicate a high diversification of solutions and effective reflection of trade-offs between conflicting criteria, and also confirm the possibility of achieving significant coalition benefit at the expense of a moderate increase in risk or cost. The proposed CoopEvo-CloudSec method demonstrates high adaptability to the changing risk profile of the cloud environment, ensuring a balance between productivity, cost-effectiveness, security and collective benefit from the cooperation of defenders. The model is described in the form of formalized mathematical expressions, pseudocode, and algorithm flowchart, which makes it suitable for further software implementation and practical application in real cloud infrastructures.

Keywords: cloud computing, resource allocation, cybersecurity, game theory, cooperative games, coalition games, evolutionary optimization, NSGA-II, dynamic risk, multi-criteria optimization.

REFERENCES

1. Mykhailiv, V. I. (2015). Experimental Studies of Information Technology for Data Protection in Cloud Computing Systems. *Current Problems of Automation and Information Technologies, 19*, 52–66.
2. Tsyrkaniuk, D. (2025). A Model for the Distribution of Computational Tasks in Cloud Infrastructure Incorporating Performance, Cost, And Security Considerations. *Cybersecurity Education Science Technique, 4(28)*, 619–632. https://doi.org/10.28925/2663-4023.2025.28.836
3. Qin, S., Pi, D., Shao, Z., & Xu, Y. (2023). A Cluster-based Cooperative Co-Evolutionary Algorithm for Multiobjective Workflow Scheduling in a Cloud Environment. *IEEE Transactions on Automation Science and Engineering, 20(3)*, 1648–1662. https://doi.org/10.1109/tase.2022.3183681
4. Tan, B., H., Mei, Y., & Zhang, M. (2020). A Cooperative Coevolution Genetic Programming Hyper-Heuristics Approach for On-Line Resource Allocation in Container-Based Clouds. *IEEE Transactions on Cloud Computing, 10(3)*, 1500–1514. https://doi.org/10.1109/tcc.2020.3026338
5. Goudarzi, S., Soleymani, S., Wang, W., & Xiao, P. (2023). UAV-Enabled Mobile Edge Computing for Resource Allocation Using Cooperative Evolutionary Computation. *IEEE Transactions on Aerospace and Electronic Systems, 59*, 5134–5147. https://doi.org/10.1109/taes.2023.3251967

6. Goudarzi, P., Hosseinpour, M., & Ahmadi, M. (2020). Joint Customer/Provider Evolutionary Multi-objective Utility Maximization in Cloud Data Center Networks. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 45(2)*, 479–492. https://doi.org/10.1007/s40998-020-00381-x
7. Guzek, M., Bouvry, P., & Talbi, E.-G. (2015). A Survey of Evolutionary Computation for Resource Management of Processing in Cloud Computing. *IEEE Computational Intelligence Magazine, 10(2)*, 53–67. https://doi.org/10.1109/mci.2015.2405351
8. Atwal, S., Singh, D., & Chhabra, A. (2025). Resource Allocation Strategies for Edge and Fog Computing in the Cloud Continuum. In *2025 Int. Conf. on Intelligent Control, Computing and Communications (IC3)*, 208–213. https://doi.org/10.1109/ic363308.2025.10957263
9. Du, J., Jiang, C., Benslimane, A., Guo, S., & Ren, Y. (2021). SDN-based Resource Allocation in Edge and Cloud Computing Systems: An Evolutionary Stackelberg Differential Game Approach. *IEEE/ACM Transactions on Networking, 30(4)*, 1613–1628. https://doi.org/10.1109/tnet.2022.3152150
10. Fan, W., Zhao, L., Liu, X., Su, Y., Li, S., Wu, F., & Liu, Y. (2024). Collaborative Service Placement, Task Scheduling, and Resource Allocation for Task Offloading With Edge-Cloud Cooperation. *IEEE Transactions on Mobile Computing, 23(1)*, 238–256. https://doi.org/10.1109/tmc.2022.3219261
11. Choi, J., Choi, C., Lynn, H. M., & Kim, P. (2015). Ontology based APT Attack Behavior Analysis in Cloud Computing. In *2015 10th Int. Conf. on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp. 375–379). IEEE. https://doi.org/10.1109/bwcca.2015.69
12. Alshaikh, A., Alanesi, M., Yang, D., & Alshaikh, A. (2023). Advanced Techniques for Cyber Threat Intelligence-based APT Detection and Mitigation in Cloud Environments. In *Int. Conf. on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023)* (Vol. 12718, pp. 147–157). SPIE. https://doi.org/10.1117/12.2681627
13. Shabala, Y., & Korniichuk, B. (2024). Methodology for Assessing IoT Security at Industrial Facilities. *Management of Development of Complex Systems, 60*, 146–155. https://doi.org/10.32347/2412-9933.2024.60.146-155
14. Stefurak, O. R., Tykhonov, Yu. O., Laptyev, O. A., & Zozulya, S. A. (2020). Improving the Stochastic Model to Identify Threats of Damage or Unauthorized Leakage. *Modern Information Security, 2*, 19–26. https://doi.org/10.31673/2409-7292.2020.021926
15. Li, B., Chen, Y., Huang, S., Yao, R., Xia, Y., & Mei, S. (2019). Graphical Evolutionary Game Model of Virus-based Intrusion to Power System for Long-Term Cyber-Security Risk Evaluation. *IEEE Access, 7*, 178605–178617. https://doi.org/10.1109/access.2019.2958856
16. Zhang, H., Tan, J., Liu, X., Huang, S., Hu, H., & Zhang, Y. (2022). Cybersecurity Threat Assessment Integrating Qualitative Differential and Evolutionary Games. *IEEE Transactions on Network and Service Management, 19(3)*, 3425–3437. https://doi.org/10.1109/tnsm.2022.3166348
17. Höfer, C. N., & Karagiannis, G. (2011). Cloud Computing Services: Taxonomy and Comparison. *Journal of Internet Services and Applications, 2(2)*, 81–94. https://doi.org/10.1007/s13174-011-0027-x
18. Li, P., & Yang, X. (2019). On Dynamic Recovery of Cloud Storage System under Advanced Persistent Threats. *IEEE Access, 7*, 103556–103569. https://doi.org/10.1109/access.2019.2932020
19. Winter, E. (2002). Chapter 53 The shapley value. In Handbook of Game Theory with Economic Applications (pp. 2025–2054). Elsevier. https://doi.org/10.1016/s1574-0005(02)03016-3
20. Faigle, U., & Kern, W. (1992). The Shapley Value for Cooperative Games under Precedence Constraints. *International Journal of Game Theory, 21*, 249–266.
21. Golovanenko, M. (2012). Application of Cooperative Game Theory for the Development of Corporate Social Responsibility. *Ukraine: Aspects of Labor, 2*, 47–50.
22. Pavlov, I. M., & Tolyupa, S. V. (2014). Analysis of Approaches to Modeling Decision-making Processes in the Design of Information Security Systems. *Modern Information Security, 2*, 96–104.