© Yaskevych Y. Research of the method for selecting security tools in distributed information systems // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 19-26. © This is an open access article under the* CC BY 4.0 International license.

DOI: 10.18372/2225-5036.32.21642

ДОСЛІДЖЕННЯ МЕТОДУ ВИБОРУ ЗАСОБІВ ЗАХИСТУ РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

Юрій Яскевич

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна



ЯСКЕВИЧ Юрій Владиславович, аспірант,
Рік та місце народження: 1996 рік, м. Київ, Україна
Освіта: Державний університет телекомунікацій.
Наукові інтереси: Стійкість інформаційних мереж, криптографічні примітиви, аналіз методів злому шифрів
Публікації: наукові публікації, серед яких монографії, наукові статті та тези, матеріали доповідей на конференціях.
E-mail: y.yaskevych.asp@kubg.edu.ua
Orcid ID: 0009-0005-6084-5229

Анотація. *Стаття присвячена розв'язанню релевантної науково-практичної задачі обґрунтування вибору засобів захисту (ЗЗІ) розподілених інформаційних систем (РІС), які функціонують в умовах жорстких ресурсних обмежень та активного кібернетичного протиборства. Метою дослідження є експериментальна верифікація ефективності, адекватності та працездатності розробленого ігрово-оптимізаційного методу, який поєднав теоретико-ігровий апарат для моделювання дій сторін та методи багатокритеріальної оптимізації. Методологічну основу дослідження склали серії обчислювальних експериментів (ОбЕк), реалізовані на базі авторського програмного комплексу. Експерименти включали генерацію синтетичних топологій РІС, які враховують гетерогенність вузлів РІС, моделювання сценаріїв атак раціонального зловмисника та пошук захисних конфігурацій за допомогою еволюційного алгоритму NSGA-II. Здійснено порівняльний аналіз запропонованого методу з поширеними евристичними стратегіями розподілу ресурсів, як-от пріоритет критичності, захист вразливостей, випадковий вибір тощо. Результати моделювання експериментально підтвердили висунуті гіпотези. Доведено, що врахування топології мережі та каскадних ефектів поширення шкоди є доцільним для синтезу стійкої системи захисту. Підтверджено ефективність застосування багатокритеріальної оптимізації. Побудова фронту Парето у просторі «ризик – вартість – рівень покриття» дозволила виявити множину недомінованих рішень, які за сукупністю показників перевершують однокритеріальні моделі. Кількісний аналіз результатів засвідчив статистично значущу перевагу розробленого методу. Зокрема, встановлено, що ігрово-оптимізаційні стратегії забезпечили зниження інтегрального ризику РІС на 56–58 % відносно початкового рівня, тоді як базові та спрощені моделі продемонстрували результат лише у межах 48–55 %. Середній показник залишкового інтегрального ризику для запропонованого методу склав 0,42, що суттєво краще за показники базових стратегій, які варіювалися від 0,44 (для гнучких евристик) до 0,52 (для стратегій пріоритету критичності). Абсолютне зменшення ризику відносно найгіршого сценарію склало 0,10.*

Ключові слова: *розподілені інформаційні системи, кібербезпека, вибір засобів захисту, багатокритеріальна оптимізація, NSGA-II, теорія ігор, оцінка ризиків, обчислювальний експеримент.*

Вступ

Чинні розподілені інформаційні системи (далі РІС) мають складну архітектуру, велику кількість гетерогенних елементів, що робить їх вразливими до широкого кола кібернетичних загроз. В умовах обмеженого бюджету на кібербезпеку перед адміністраторами РІС постає нетривіальне завдання - як обрати такий набір засобів захисту інформації (ЗЗІ), який би мінімізував ризики при прийнятних витратах. Ситуація ускладнена тим, що дії зловмисника часто мають стратегічний характер. Сторона атаки гнучко підлаштовується до побудованого захисту РІС. У попередніх роботах [1, 2] запропоновано ігрово-оптимізаційну модель розв'язання цієї задачі. Дана стаття присвячена практичній верифікації цієї моделі шляхом проведення серії обчислювальних експериментів (ОбЕк), спрямованих на підтвердження ефективності запропонованого методу порівняно з евристичними стратегіями захисту.

Постановка проблеми

Ефективний захист РІС вимагає врахування не лише вартості та захисних властивостей окремих ЗЗІ, але й топології РІС, критичності вузлів та каскадних ефектів поширення шкоди. Чинні методи та моделі вибору ЗЗІ спираються або на експертні оцінки, або на спрощені евристики, як-от пріоритетний захист найважливіших вузлів, ігноруючи варіативність стратегій нападника. Проблема полягає у відсутності експериментально підтверджених методик, які б дозволяли знаходити Парето-оптимальні конфігурації захисту в умовах протидії раціонального або обмежено-раціонального противника. Необхідно дослідити, наскільки застосування складного математичного апарату [1] (ігрова теорія та багатокритеріальна оптимізація) виправдовує себе на

© Yaskevych Y. Research of the method for selecting security tools in distributed information systems // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 19-26. © This is an open access article under the* CC BY 4.0 International license.

практиці порівняно з простішими методами розподілу ресурсів.

Огляд попередніх досліджень

Питання оптимального вибору контрзаходів розглянуто у багатьох роботах останніх років [1-14]. Так ігрові моделі Léveillé D., Jaskolka [9] та J.Lye K. W., Wing J. M [13], дослідили ігрові стратегії в мережевій безпеці. Проте ці моделі складні для масштабування на великі РІС. В ооптимізаційній моделі Dewri R. та інших [10] автори застосовували багатокритеріальну оптимізацію на деревах атак. В [8], а Gao X. С колегами використали методи Q-Learning для оптимізації. Однак ці роботи не враховували топологічні особливості РІС. Дослідження Cavusoglu H. [11] та Gupta R. [12] сфокусовані на фінансовій ефективності інвестицій в захист. Але ці роботи розглядали систему як «чорну скриньку» без деталізації вразливостей окремих вузлів РІС.

Зазначимо, що автором в [1] запропоновано метод, який поєднав ігровий апарат з еволюційною оптимізацією. Поточна стаття є логічним продовженням досліджень й сфокусована на його експериментальній перевірці.

Мета дослідження

Метою статті є перевірка працездатності, адекватності та ефективності розробленого ігрово-оптимізаційного методу вибору засобів захисту РІС шляхом проведення обчислювальних експериментів.

Для досягнення мети вирішуються такі завдання:

- верифікація етапів методу та аналіз впливу обмеженості ресурсів на очікувані втрати РІС;
- дослідження впливу структури РІС та критичності вузлів на оптимальний склад ЗЗІ;
- порівняння отриманих Парето-оптимальних рішень із результатами застосування базових евристичних стратегій захисту РІС;
- кількісна оцінка виграшу в зниженні інтегрального ризику при використанні запропонованого методу.

Результати дослідження

Обчислювальні експерименти (далі по тексту ОбЕк) проведені з метою перевірки працездатності, адекватності та ефективності розробленого ігрово-оптимізаційного методу вибору засобів захисту РІС систем в умовах цілеспрямованої протидії з боку раціонального або обмежено-раціонального противника, див. [1]. Основними завданнями експериментальних досліджень є: аналіз впливу обмеженості ресурсів сторони захисту на очікувані втрати РІС; дослідження варіацій варіантів ЗЗІ відповідно до структури РІС та критичності її вузлів для пошуку оптимального складу ЗЗІ; оцінювання ролі стратегічної поведінки нападника у формуванні оптимальних конфігурацій захисту РРІ; порівняння отриманих рішень із спрощеними стратегіями захисту.

Метою ОбЕк є покрокова верифікація кожного етапу методу [1], а також оцінювання його інтегральних властивостей у вигляді Парето-оптимальних конфігурацій захисту РІС або окремих вузлів за умов стратегічної протидії.

Загальну структура ОбЕк подано в таблиці 1.

Таблиця 1

Загальна структура обчислювального експерименту

№ етапу методу [1]	Назва етапу методу	Інтерпретація в експерименті
1	Формалізація структури РІС	Генерація тестових топологій РІС
2	Оцінювання критичності компонентів	Формування векторів (ω_v)
3	Формування множини ЗЗІ	Побудова простору альтернатив
4	Ресурсні обмеження	Обмеження допустимих конфігурацій
5	Модель зловмисника	Генерація сценаріїв атак
6	Моделювання шкоди	Обчислення локальних і мережевих втрат РІС
7	Формування критеріїв	Побудова вектора (J_z)
8	Ігрове оцінювання	Мінімаксні та баєсівські оцінки.
9–10	Багатокритеріальна оптимізація	Наближення фронту Парето
11	Постобробка	Вибір компромісного рішення

Для практичної реалізації запропонованого у [1] методу та проведення ОбЕк розроблено програмний продукт (ПП) на мові Python. Модульна архітектура комплексу дозволила реалізувати всі етапи методу, зазначені в 1. Також модульна структура ПП забезпечила потенціал гнучкої зміни параметрів ОбЕк. Загальна структура ПП представлена на рис. 1.

ПП складався з трьох основних модулів. Модулі відповідали етапам методу. Перший модуль – це модуль генерації тестових даних РІС (generate_ris_dataset.py). Модуль реалізував етапи 1 – 4 методу (див. табл. 1) та відповідав за формування множини тестових моделей РІС та простору альтернатив захисту РІС. Модуль генерував

синтетичні дані. Зазначимо, що дані прийнято на підставі типових значень для реальних РІС. При застосуванні ПП у практичних кейсах дані датасету заміняємо на реальні дані для РІС, який досліджуємо. Модуль формує:

– орієнтовані графи топології РІС – генеруємо масштабно-вільні РІС, які імітують нерівномірний розподіл зв'язків.

– вектор важливості (критичності) вузлів. Тобто для кожного вузла v п процесі ОбЕк обчислюємо його вагу ω_v. Модуль generate_ris_dataset.py створював вузли різних типів (сервери, бази даних, IoT-пристрої тощо), див. таблицю 3.8. Кожному з вузлів присвоюємо значення критичності на основі його типу та ролі в мережі. Це забезпечувало під час проведення ОбЕк асиметричний розподіл важливості вузлів;

– дискретний простір альтернатив захисту. Формуємо каталог засобів ЗЗІ – K. Кожен засіб k мав атрибути: тип – превентивний, детекційний; вартість впровадження на вузол $c_{v,k}$; ефективність.

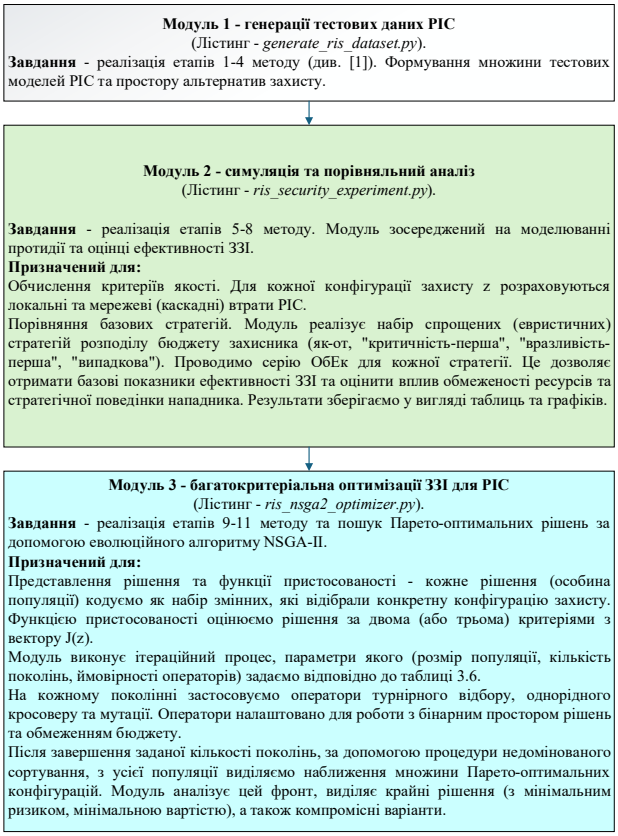


Рис. 1. Структура ПП для проведення ОбЕк

Експеримент проводився у послідовності, яка відповідала логіці нашого методу, див. [1]. Спочатку запускався модуль генерації датасету. Він створював конкретні сценарій РІС. Це відповідало етапам 1 – 4. Далі отриманий датасет передаємо модулю симуляції. Він проводив порівняльний аналіз базових стратегій сторін та оцінював вихідний рівень ризиків для РІС – етапи 5 – 8. На основі цих результатів можемо скоригувати у разі потреби параметри бюджету та інші обмеження. Потім управління передаємо модулю оптимізації NSGA-II. Отже, це фінальний модуль виконував пошук Парето-оптимальних конфігурацій для заданого сценарію – етапи 9 – 11). Завершальним кроком роботи нашого ПП є інтеграція та інтерпретація результатів з усіх модулів. На цьому етапі реалізуємо порівняння рішень, які знайдені на підставі [1], з базовими стратегіями сторін, аналіз отриманого Парето-фронту та формування остаточних рекомендацій щодо вибору ЗЗІ. Зазначимо, що проведені нами обчислювальні експерименти спрямовані на перевірку наступних основних експериментальних гіпотез.

Гіпотеза 1 (Н1) – урахування стратегічної поведінки раціонального або обмежено-раціонального противника в межах ігрово-оптимізаційної моделі дозволить зменшити очікувані втрати РІС порівняно зі спрощеними (евристичними) стратегіями захисту, які не враховували варіативність стратегій сторони атаки.

Гіпотеза 2 (Н2) – оптимальний склад та розміщення засобів захисту істотно залежать від мережевої структури РІС й неоднорідності її важливих вузлів, що підтверджує доцільність урахування каскадних ефектів поширення шкоди для РІС.

Гіпотеза 3 (Н3) – багатокритеріальна оптимізація у просторі «ризик – вартість – рівень покриття» сформує множину Парето-оптимальних конфігурацій ЗЗІ для РРІ, які забезпечать найкращий компроміс між безпекою та ресурсними витратами порівняно з однокритеріальними методами вибору ЗЗІ.

Перевірку зазначених гіпотез здійснюємо на основі кількісного аналізу результатів ОбЕк, наведених у наступному параграфі.

Оскільки ОбЕк містили стохастичні компоненти, як-от генерація топологій РІС, параметрів атак, а також еволюційні оператори алгоритму NSGA-II, для підвищення достовірності результатів експериментальні серії проводилися з урахуванням повторюваності. А саме, для кожного сценарію РІС виконувалася серія незалежних прогонів із фіксованими або контрольованими початковими параметрами генерації. Отримані результати аналізувалися з використанням усереднених значень показників ефективності. Це дозволило зменшити вплив випадкових флуктуацій та оцінити стійкість знайдених Парето-оптимальних рішень. Також, зазначимо, що проведені ОбЕк мали низку обмежень. Зокрема, в роботі використовувався згенеровані сценарії роботи РІС. Його параметри відповідали типовим значенням, характерним для РІС. Разом з тим, у практичних кейсах застосування структура РІС та параметри загроз матимуть власні особливості.

Також, множина атак і засобів захисту, яка розглядалася у ОбЕк, є скінченною та репрезентувала найбільш поширені класи загроз і засобів протидії. Розширення цієї множини не змінить загальної логіки запропонованого методу.

© Yaskevych Y. Research of the method for selecting security tools in distributed information systems // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 19-26. © This is an open access article under the* CC BY 4.0 International license.

Проведення експериментів здійснювалося відповідно до етапів методу, узагальнено представлених у [1, 2], та включало послідовне формування структури PIP, задання параметрів вузлів і каналів взаємодії, моделювання можливих атак і засобів захисту, а також подальший пошук Парето-оптимальних конфігурацій системи захисту. Першим етапом ОбЕк є генерація структури PIC. В експерименті PIC розглядаємо як зважений граф, див. рис. 2, як один з прикладів.

Вершини графа відповідали функціональним вузлам PIC. Ребра графа – інформаційні або мережеві зв'язки між вузлами. Граф дозволив нам під час ОбЕк врахувати специфіку PIC та вплив структурних параметрів мережі на процеси поширення атак і ефективність застосування ЗЗІ.

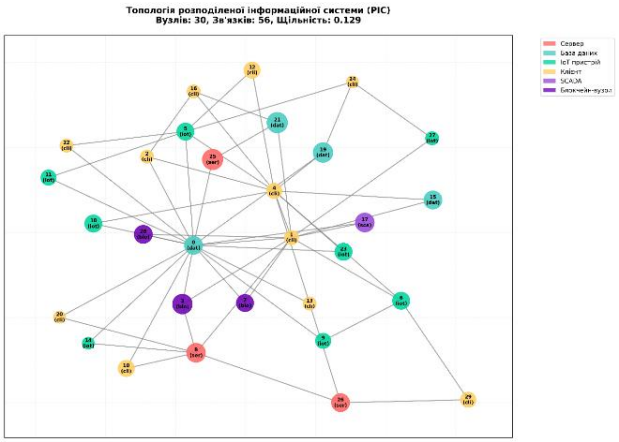


Рис. 2. Приклад топології PIC для одного обчислювального експерименту

Для забезпечення репрезентативності експериментів структуру PIC формуємо синтетично на основі стохастичної моделі. Ця модель відтворювала типові властивості реальних PIC. Зокрема, враховано неоднорідність вузлів, наявність високо зв'язаних компонентів та різну важливість елементів PIC. Згенерована на рис. 2 топологія використовувалась під час ОбЕк як базове середовище для подальшого аналізу стратегічної взаємодії між захисником і противником. А також для вибору ЗЗІ. Подальший виклад результатів у цьому параграфі структуровано відповідно до логіки запропонованого методу. На рис. 2 наведено приклад топології PIC, яка містить 30 вузлів та 56 зв'язків. Та щільність графа на рис. 2 становила 0,129. Значення щільності є характерним для PIC та відображало відсутність повнозв'язної структури, яка зумовлює наявність вузлів з різною мережею впливу та різними потенційними наслідками компрометації під час атак. На рис. 2 структура PIC є гетерогенною за функціональним призначенням вузлів. У системі присутні серверні вузли, вузли зберігання даних, клієнтські вузли, IoT-пристрої, компоненти типу SCADA, а також блокчейн-вузли. Отже, різноманітність вузлів віддзеркалила чинні тенденції синтезу PIC і створила належні передумови для формування неоднорідного простору загроз і засобів захисту.

Зазначимо, що для більшої зручності та наочності основні результати, як-от графіки, отримані під час ОбЕк, зведено на дашборд. Наприклад один з дашборд наведено на рис. 3. Стратегії захисту відрізнялися принципами прийняття рішень. Отже, ми використовуємо:

евристичні методи. Вони базувалися на локальних параметрах вузлів –важливість та/або вразливість;

оптимізаційні методи та стратегії. Ці стратегії, першочергово орієнтовані на мінімізацію ризику, а також на або максимізацію ефективності використання ресурсів стороною захисту.

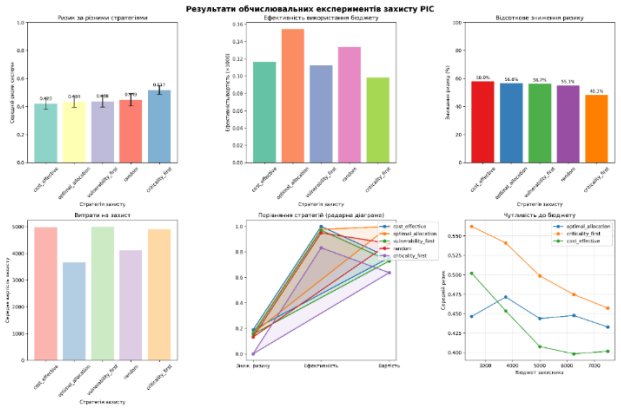


Рис. 3. Дашборд з результатами ОбЕк, отриманих в процесі аналізу стратегій сторони захисту PIC

Сукупність представлених на рис. 3 показників охоплювала як абсолютні метрики, як-от середній ризик системи, витрати на захист, так і відносні характеристики – відсоткове зниження ризику, ефективність використання бюджету на захист PIC. Отже, для ОПР вивід результатів саме на дашборд давав змогу всебічно оцінити наслідки застосування кожної зі стратегій.

Аналіз отриманих розподілів дозволив виділити чітку ієрархію ефективності методів. Базова стратегія «Random» (випадковий розподіл ресурсів, показана на рис. 3 червоним кольором) очікувано продемонструвала є найвищий рівень залишкового ризику. Результат пояснимо ігноруванням специфіки топології PIC та параметрів цінності активів. Евристичні стратегії «Criticality First» (пріоритет критичних вузлів – показано блакитним кольором) та «Vulnerability First» (пріоритет вразливих вузлів – фіолетовий колір) показали кращі результати. Рівень ризику зменшено. Однак їхня ефективність обмежена локальним характером прийняття рішень. Рішення не враховували критерій «ефективність ЗЗІ / вартість». Найвищу результативність мала стратегія «Optimal Allocation» (жовтий стовпчик гістограми на рис. 3). Як бачимо на гістограмі, застосування розробленого методу дозволило досягти найнижчого показника R_{sys}.

© Yaskevych Y. Research of the method for selecting security tools in distributed information systems // *Ukrainian Scientific Journal of Information Security, 2026, vol. 32, issue 1, pp. 19-26. © This is an open access article under the* CC BY 4.0 International license.

Кількісна оцінка розриву в ефективності засвідчила, що оптимізаційні заходи перевершили найкращу з евристик «Cost Effective» на 12–18% (залежно від ітерації ОбЕк). А стратегію випадкового вибору перевершило майже вдвічі.

Далі, відповідно до логіки нашого методу [1], на наступному етапі ОбЕк ми розглянули розв'язання задачі багатокритеріальної оптимізації конфігурації ЗЗІ для РІС із використанням еволюційного алгоритму NSGA-II. Метою оптимізації є одночасне мінімізування інтегрального ризику системи R_{int} (зауважимо, що в нашому тлумаченні інтегральний ризик РІС (R_{int}) – узагальнене значення ризику функціонування РІС, отримане шляхом агрегування локальних ризиків її компонентів відповідно до [1], а також згідно [15 – 17]) та вартості ЗЗІ при максимізації ефективності використання ресурсів стороною захисту. Як і на попередньому етапі для зручності сприяння результати виводимо на дашборд, див. рис. 4. Також результати зберігаймо для кожного ОбЕк в окрему теку.

На підграфіку «Парето-фронт оптимальних рішень» (див. верхній лівий кут дашборда на рис. 4), представлено множину недомінованих рішень, які формують Парето-оптимальний фронт у просторі критеріїв «вартість захисту – ризик системи». Отриманий фронт мав спадний характер. Це підтвердило наявність типового компромісу між фінансовими витратами та рівнем безпеки РІС. Тобто зменшення ризику досягнуто для нашої РІС шляхом зростання вартості захисних заходів по вузлах.

Окремо на цьому графіку виділені рішення з мінімальним ризиком (червона зірка). Це рішення забезпечило найнижче значення інтегрального ризику, проте воно характеризувалося максимальною вартістю (B) захисту РІС.

Підграфік «Топ-10 рішень за ризиком», див. верхній правий кут дашборда на рис. 4 віддзеркалив ранжування оптимальних рішень за зростанням інтегрального ризику (див. вираз 1). Аналіз показав, що найкращі рішення забезпечили значення ризику в інтервалі приблизно 0,23 – 0,32. Це нижче за базовий рівень ризику системи без захисту. При цьому навіть серед топ-10 рішень спостерігаємо для топології РІС на рис. 2, різницю у вартості та структурі конфігурацій. Це довело доцільність використання Парето-аналізу замість вибору єдиного «глобально оптимального» рішення.

Підграфік «Залежність ризику від кількості засобів», див. лівий нижній кут дашборда на рис. 4, ілюстрували вплив кількості застосованих ЗЗІ на рівень інтегрального ризику [15 – 17].

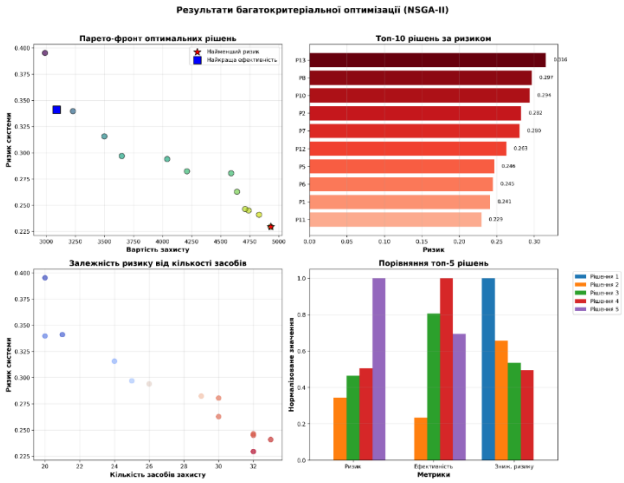


Рис. 4. Дашборд для другого етапу обчислювальних експериментів

(Результати багатокритеріальної оптимізації ЗЗІ для РІС)

Отже, згідно [15 – 17] інтегральний ризик визначаємо в наших ОбЕк так:

$$R_{int} = \sum_{i=1}^{N} \omega_i \cdot R_i \,, \qquad (1)$$

де R_{int} –інтегральний ризик ІБ для РІС; R_i – локальний ризик порушення безпеки i-го вузла або компонента системи; ω_i – ваговий коефіцієнт, що відображав важливість i-го вузла ($\sum \omega_i = 1$); N – кількість вузлів РІС.

Завершальним етапом ОбЕк став порівняльний аналіз результатів, отриманих за допомогою запропонованого багатокритеріального методу оптимального вибору ЗЗІ на основі алгоритму NSGA-II, з результатами застосування базових евристичних стратегій розподілу захисних ресурсів, див. рис. 5. Мета етапу – це верифікація практичної доцільності запропонованого методу та кількісна оцінка його переваг.

Аналіз показників інтегрованого ризику (R_{int}) засвідчив, що всі базові стратегії продемонстрували вищі значення ризику ІБ РІС порівняно з найкращими та середніми рішеннями, які ми отримали за допомогою алгоритму NSGA-II. При цьому навіть найуспішніша з базових стратегій не досягла рівня зниження ризику (R_{int}), який забезпечено оптимальними конфігураціями ЗЗІ, сформованими еволюційним алгоритмом.

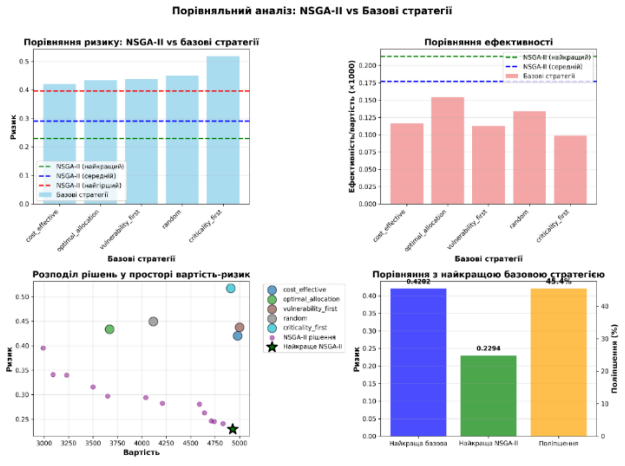


Рис. 5. Фінальний дашборд із результатами обчислювальних експериментів

Отриманий на дашборд, див. рис. 5, результат підтвердив, що евристичні методи формування стратегій захисту PIC, які орієнтовані на один домінуючий критерій, як-от вартість, вразливість або критичність тощо, не дозволять стороні захисту повною мірою врахувати складну структуру взаємозв'язків між елементами PIC та варіативну поведінку противника. Порівняння ефективності, тобто відношення досягнутого зниження ризику (R_{int}) до витрачених ресурсів на захист PIC, довело, що рішення, отримані в межах багатокритеріальної оптимізації, сформували значно вищу межу ефективності порівняно з базовими стратегіями. Навіть середні за якістю рішення NSGA-II перевищували більшість евристичних методів. Отже, це довело стабільність роботи нашого методу та його низьку чутливість до випадкових факторів. На відміну від базових стратегій, запропонований в [1, 2] метод дозволив нам під час проведення ОбЕк сформувати множину альтернативних рішень із керованим компромісом між ризиком (R_{int}) і вартістю ЗЗІ для PIC. Отже, це розширює потенціал можливості прийняття обґрунтованих управлінських рішень з завдані кібербезпеки PIC.

Резюмуючи аналіз результатів фінального етапу ОбЕк, наголосимо наступне. За підсумками більш ніж 50 ОбЕк сформовано обмежену множину альтернативних конфігурацій захисту PIC. Ця множина мала різні параметри узгодженості між рівнем безпеки PIC, вартістю реалізації та структурною насиченістю засобами захисту. У межах експерименту отримано від 10 до 13 Парето-оптимальних рішень для топології PIC, яку ми раніше навели на рис. 2. Рішення охоплювали широкий діапазон значень ризику (R_{int}) та фінансових витрат на ЗЗІ PIC. Аналіз отриманих рішень показав, що мінімальне значення ризику (R_{int}) досягнуто шляхом концентрації ЗЗІ на критичних вузлах PIC та збільшення загальної кількості застосованих засобів захисту. Водночас ідентифіковано рішення з помірними витратами. Ці рішення забезпечуваои в наших ОбЕк прийнятну ефективність використання ресурсів стороною захисту. Своєю чергою це важливо у сценаріях протистояння із зловмисниками, які не мають жорстких бюджетних обмежень на здійснення атаки.

Порівняльний аналіз із базовими евристичними стратегіями, підтвердив значну перевагу застосування еволюційної компоненти нашого методу. Найкраща з базових стратегій продемонструвала значно вищий рівень залишкового ризику порівняно з оптимальними рішеннями NSGA-II. Отже, результат засвідчив обмеженість методик, які орієнтовані на окремі локальні критерії захисту PIC без урахування їх взаємного впливу. Отримані результати також засвідчили, що використання Парето-фронту дозволяє ОПР, обрати рішення тобто конфігурацію ЗЗІ відповідно до пріоритетів конкретного сценарію експлуатації PIC. Це можуть бути сценарії мінімізації ризику, обмеження витрат або досягнення компромісу між цими показниками. Отже, запропонований метод забезпечив в нашому дослідження не лише формальну оптимальність, а й гнучкість практичного застосування в умовах варіативної стратегічної протидії з боку раціонального або обмежено-раціонального противника.

Загалом результати ОбЕк підтвердили доцільність застосування багатокритеріальної оптимізації для задач вибору засобів захисту PIC.

Для коректного позиціювання нашого методу та отриманих під час проведення ОбЕк результатів доцільно порівняти всі раніше виявлені в [2] методи за наступними критеріями: математичний апарат; модель системи (PIC), тобто чи враховує модель топологію й каскадні ефекти під час атаки на PIC; модель загрози, тобто чи маємо ми справу з варіативним чи раціональним нападником; чи враховує метод або модель показники ймовірності реалізації певних етапів атаки на PIC; багатокритеріальність, тобто чи будуємо фронт Парето. Або це звичайна згортка в один критерій.

Висновки

Результати обчислювальник експериментів (ОбЕк) підтвердили гіпотезу H1 щодо доцільності урахування стратегічної поведінки противника, який атакує PIC. Встановлено, що ігрово-оптимізаційні стратегії забезпечують істотніше зменшення очікуваних втрат PIC порівняно зі спрощеними методиками, які не враховують варіативність дій сторони атаки. Підтверджено експериментально гіпотезу H2 про залежність оптимального складу та розміщення ЗЗІ від топологічної структури PIC та неоднорідності її вузлів. Урахування критичності елементів та мережевих ефектів поширення шкоди дозволило сформувати конфігурації захисту, стійкі до каскадних атак і латерального переміщення порушника в межах PIC, чого неможливо досягти в моделях з ізольованим розглядом компонентів. Аналіз множин Парето-оптимальних рішень підтвердив

гіпотезу Н3 щодо ефективності багатокритеріальної оптимізації у просторі «ризик – вартість – рівень покриття». Отримані Парето-фронти продемонстрували наявність компромісних рішень, які перевершували однокритеріальні та евристичні стратегії за сукупністю показників. Результати ОбЕк створили підґрунтя для гнучкого вибору захисної конфігурації відповідно до пріоритетів особи, яка приймає рішення (ОПР).

Доведено практичну корисність методу. Зокрема, реалізація ОбЕк на основі еволюційного багатокритеріального алгоритму NSGA-II підтвердила можливість ефективного наближення множини Парето-оптимальних рішень навіть для РІС середнього та великого розміру. Отримані результати засвідчили, що застосування еволюційних методів є обґрунтованим компромісом між якістю рішень та обчислювальною складністю задачі. Встановлено за результатами серії ОбЕк, що застосування запропонованого методу дозволяє зменшити середній інтегральний ризик РІС до рівня 0,42, тоді як для базових стратегій цей показник варіювався від 0,44 (для евристик) до 0,52 (для стратегій пріоритету критичності). Абсолютне зменшення середнього ризику системи відносно найгіршого сценарію становило 0,10. Результат є статистично значущим для сценаріїв з обмеженим бюджетом захисту РІС. Відносна ефективність запропонованого методу підтверджена показниками відсоткового зниження інтегрального ризику: оптимізаційні та економічно орієнтовані стратегії забезпечили зниження ризику на 56–58 % відносно вихідного рівня, тоді як випадкові або спрощені моделі продемонстрували зменшення у межах 48–55 %. Отже, доведено, що навіть за однакових ресурсних обмежень раціональний вибір і розподіл ЗЗІ має вирішальний вплив на досягнутий рівень безпеки РІС.

Список літератури

[1] Яскевич, Ю. (2025). Ігрово-оптимізаційна модель вибору засобів захисту розподілених інформаційних систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30), 715–726. https://doi.org/10.28925/2663-4023.2025.30.913

[2] Яскевич Ю. (2026). Розподілені інформаційні системи як об’єкт кіберзахисту та загрози їхньої безпеки. Телекомунікаційні та інформаційні технології, 1(90)

[3] Лєнков, С., Джулій, В., Муляр, І., Лєнков, Є., & Кольцов, Р. (2025). Оцінки ефективності системи захисту конфіденційної інформації розподілених інформаційних систем. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29), 628-644.

[4] Геряк, Ю., & Берко, А. (2024). Система критеріїв оцінки якості даних в розподілених інформаційних системах. Інформаційні системи та мережі.–2024.– Вип, 16, 191-202.

[5] Божко, В. І., & Охріменко, О. Г. (2006). Методика оцінки функціональної стабільності структури розподіленої інформаційної системи критичного застосування. Радіоелектронні і комп’ютерні системи, (7), 68-71.

[6] Романів, Р. С., & Бандурка, О. І. (2024). Методи забезпечення функціональної стійкості розподілених інформаційних систем моніторингу руху транспортних засобів за допомогою технології блокчейн. Information technologies and automation–2024, 221.

[7] Палко Д.В., Мирутенко Л.В. Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем. Ukrainian Information Security Research Journal, 26(2), 236-252.

[8] Gao, X., Zhou, Y., Xu, L., & Zhao, D. (2022). Optimal security protection strategy selection model based on Q-Learning Particle Swarm Optimization. Entropy, 24(12), 1727.

[9] Léveillé, D., & Jaskolka, J. (2024). A game-theoretic approach for security control selection. arXiv preprint arXiv:2410.22762.

[10] Dewri, R., Poolsappasit, N., Ray, I., & Whitley, D. (2007, October). Optimal security hardening using multi-objective optimization on attack tree models of networks. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 204-213).

[11] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

[12] Gupta, R., Biswas, B., Biswas, I., & Sana, S. S. (2021). Firm investment decisions for information security under a fuzzy environment: a game-theoretic approach. Information & Computer Security, 29(1), 73-104.

[13] Lye, K. W., & Wing, J. M. (2005). Game strategies in network security. International Journal of Information Security, 4(1), 71-86.

[14] Лахно, В., Криворучко, О., & Каламан, Є. (2025). Програмна реалізація вирішення задачі оптимізації вибору засобів захисту інформації на основі еволюційного алгоритму. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 257-268.

[15] ISO / IEC ISO/IEC 27005:2018. Information technology — Security techniques — Information security risk management.

[16] Hubbard, D. W. (2020). The failure of risk management: Why it's broken and how to fix it. John Wiley & Sons.

[17] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), 11-25.

УДК 004.056:519.85

Yaskevych Y. Research of the method for selecting security tools in distributed information systems

Abstract. *The article is dedicated to solving a relevant scientific and practical task of justifying the selection of information security tools (IST) for distributed information systems (DIS) operating under tight resource constraints and active cyber confrontation. The study's aim is the experimental verification of the effectiveness, adequacy, and viability of the developed game-optimization method, which combines the game-theoretic apparatus for modeling party actions with multi-criteria optimization methods.*

The methodological basis of the research consisted of a series of computational experiments implemented using proprietary software. These experiments included generating synthetic DIS topologies that account for node heterogeneity, modeling scenarios of a rational attacker's actions, and searching for optimal protective configurations using the NSGA-II evolutionary algorithm.
A comparative analysis of the proposed method was conducted against common heuristic resource allocation strategies, such as criticality priority, vulnerability protection, and random choice. The simulation results experimentally confirmed the stated hypotheses, proving that accounting for network topology and cascading damage propagation effects is essential for synthesizing a resilient defense system.
The effectiveness of multi-criteria optimization was further confirmed through the construction of a Pareto front in the "risk – cost – coverage level" space. This allowed for the identification of a set of non-dominated solutions that, in aggregate, outperform single-criterion models. Quantitative analysis of the results demonstrated a statistically significant advantage of the developed method. Specifically, it was established that game-optimization strategies provided a reduction in DIS integral risk by 56–58% relative to the initial level, while basic and simplified models demonstrated results only within the 48–55% range. The average residual integral risk for the proposed method was 0.42, which is significantly better than the performance of basic strategies, which varied from 0.44 (for flexible heuristics) to 0.52 (for criticality priority strategies). The absolute reduction in risk relative to the worst-case scenario amounted to 0.10.
Keywords: *distributed information systems, cybersecurity, selection of security tools, multi-criteria optimization, NSGA-II, game theory, risk assessment, computational experiment.*

Яскевич Юрій Владиславович, аспірант кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка.
Yurii Yaskevych, PhD Student, Department of Information and Cyber Security named after Professor Volodymyr Buryachok Borys Grinchenko Kyiv Metropolitan University.

Дата надходження:	Дата прийняття:	Дата публікації:
20.02.2026	12.03.2026	22.04.2026